National Security Agency/Central Security Service

PRESIDENTIAL TRANSITION 2009

Approved for Release by NSA on
04-13-2016, FOIA Case # 58027

Presidential Transition 2009
NSA/CSS Information Book Contents

Introduction

- Response to Request for Information from Director, National Intelligence

What We Do

- Providing and Protecting Vital Information for our Nation
- Saving Lives
  - "Intelligence Operations with the Warfighter"
  - "Key Advancements in Signals Intelligence Support: The Real Time Regional Gateway"
  - "SIGINT Contributions to Countering Terrorism"
  - "Military Intelligence Support"
  - "Countering Improvised Explosive Devices"
  - "Protecting U.S. Citizens Abroad"
- Defending Vital Networks
  - "Comprehensive National Cybersecurity Initiative (CNCI)"
  - "Maintaining Situational Awareness of Threats to Critical Federal Networks"
  - "Joint Communications Security (COMSEC) Monitoring Activity (JCMA): Support to U.S. Forces Conducting Operations in Harm's Way"
  - "Discovering Vulnerabilities in Information Systems/Information Technology Components"
  - "Industrial Partnerships – Mitigating Vulnerabilities in U.S. Information Systems "
- Advancing U.S. Goals & Alliances
  - "SIGINT Contributions to Countering Crime & Narcotics"
  - "Expanding/Broadening Signals Intelligence Foreign Partnerships"
- Protecting Privacy Rights
  - "NSA/CSS's Signals Intelligence Mission and the Protection of Privacy Rights"
  - "Oversight of NSA/CSS"
- NSA – A Unique National Asset (b)(3)-P.L. 86-36
  - "NSA/CSS Workforce"
  - "T3.0 Transformation: Strategic Plan for Technology"
  - "National Security Operations Center (NSOC) Overview"
  - "The Cryptologic Platform"
  - [redacted]
  - "Engineering the Future: The NSA/CSS Research Directorate"
  - "U.S. Nuclear Command and Control (NC2) Support"

Our Strategy for the Future

- NSA/CSS Strategic Plan
- Transformation 3.0 Overview
- Comprehensive National Cyber Initiative – Frequently Asked Questions

Our Workforce

- Workforce Overview, October 2008
- NSA/CSS Civilian Employment Plan

Our Resources and Programs

- The NSA/CSS Budget Picture – Magnitude and Focus
- NSA/CSS Acquisition Overview

Our Worldwide Enterprise

- NSA/CSS "Footprint"
- Cryptologic Center Build-out: An Administration Transition Overview
  - NSA/CSS Georgia Fact Sheets
  - NSA/CSS Hawaii Fact Sheets
  - NSA/CSS Texas Fact Sheets
  - NSA/CSS Colorado Fact Sheets
- Accesses Through Partnerships
- NSA Collection

Our Organization and Leadership

- NSA/CSS Organizational Charts
- NSA/CSS Leadership Biographies

National Security Agency
Central Security Service

Defending Our Nation. Securing The Future.

Response to DNI Request for Information

3 November 2008

Introduction

(U//~~FOUO~~) The world's information and communications increasingly reside in a rapidly changing, interconnected technological environment. Through a unique ability to operate in that environment, the National Security Agency/Central Security Service (NSA/CSS) gathers and shares unique foreign intelligence, and it protects the vital information and networks of the United States and its allies. Operating within a rigorous framework to protect legal and constitutional rights, NSA/CSS saves lives and advances America's goals and alliances.

(U//~~FOUO~~) Carrying out these missions every day, while continuously preparing for the future, is the work of a large, complex enterprise. Its scope includes tens of thousands of skilled and dedicated civilian and military personnel; an extraordinary technology base; sites around the world; and customers and partnerships throughout the Intelligence Community, the broader federal government, and beyond. This paper outlines the missions and functions, strategies, organizational structure, and relationships that enable the work of NSA/CSS. It provides a starting point and framework for a deeper understanding of this unique national asset.

Mission Statement

(U//~~FOUO~~) NSA/CSS's mission is to provide a decisive information advantage for the United States and its allies. This is accomplished through two inextricably connected missions, Signals Intelligence (SIGINT) and Information Assurance (IA), which together enable the performance of a third function – Computer Network Attack (CNA) operations:

- Through SIGINT, NSA/CSS provides foreign intelligence that gives decision-makers and warfighters access to the often-secret communications and information of adversaries and rivals.
- Where SIGINT professionals are the Nation's "codebreakers," their counterparts in the IA mission are its "codemakers." Through IA, NSA/CSS prevents unauthorized access to U.S. classified and national-security-related information and systems, while ensuring that this vital information and systems remain available to decision-makers and warfighters.
- Through enabling CNA, NSA/CSS, working with the Joint Functional Component Command for Network Warfare, enables the denial, disruption or degradation of our adversaries' information and information systems, as authorized by appropriate U.S. authorities.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

(U) Strategic Intent and Goals

(U~~//FOUO~~) NSA/CSS carries out its missions in an environment of continuous, rapid, and dramatic change. This is true of the *target* environment – for example, the difference between large nation-states, highly mobile, diffuse terrorist networks, and individual actors – and the *information* environment, characterized by the volume, velocity and variety of information on the global network. Effective operations require great capability, adaptability, and agility.

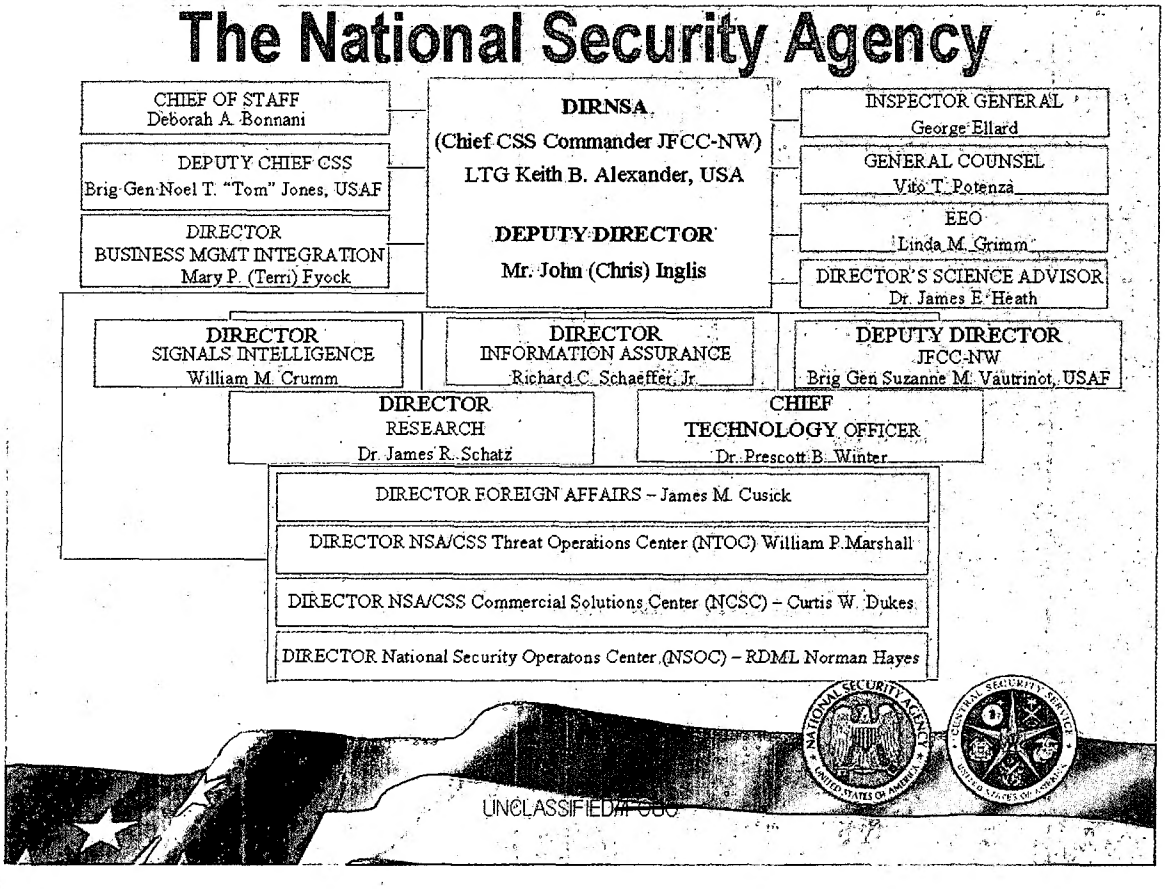
(U~~//FOUO~~) Reflecting these imperatives, the Agency's strategic intent is to accomplish its mission every day while continuously preparing for the future: modernizing its mission systems and applications, its facilities, IT and other infrastructure, growing and developing its workforce, and instituting and employing sound business management practices. The NSA/CSS Strategic Plan outlines the following four strategic goals:

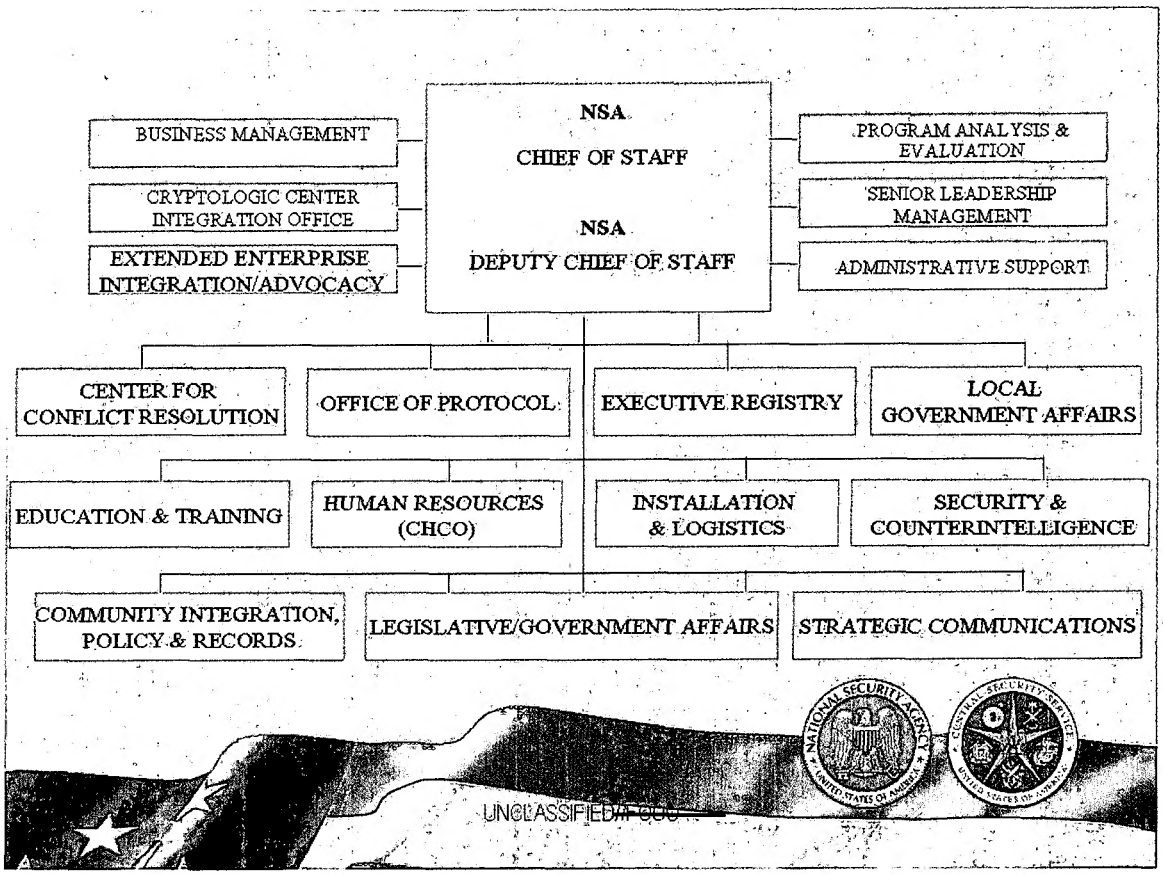
NSA/CSS STRATEGIC PLAN	
Goal 1: Mission *Deliver responsive, reliable, effective, and expert Signals Intelligence and Information Assurance, and enable Network Warfare operations, for National Security under all circumstances* • Effectively apply Signals Intelligence and Information Assurance, and enable Network Warfare operations, to defeat terrorists and their organizations at home and abroad, consistent with U.S. laws and the protection of privacy and civil liberties • Provide cryptologic services that enable partners to prevent and counter the spread of weapons of mass destruction • Avoid strategic surprise by achieving and maintaining capability and continuity against difficult targets • Protect national security systems against adversary exploitation and cyber attack • Support the global DoD mission and strengthen joint and combined military network attack operations through the provision of required intelligence and technical expertise	**Goal 2: Transformation** *Achieve global network dominance through the development and deployment of a new generation of globally distributed active and passive cryptologic capabilities* • Deliver, maintain, and operate network-enabled tools to strengthen analytic expertise, methods, and practices; tap expertise wherever it resides; and explore alternative analytic views • Develop an integrated, interoperable, distributed architecture to optimize the next generation of cryptologic systems and unify exploit, defend, and attack capabilities on the common underlying infrastructure • Develop and deploy a secure, robust information technology infrastructure to enable distributed sharing and combined operations • Exploit path-breaking scientific and research advances that will enable us to maintain and extend intelligence advantages against emerging threats
Goal 3: People *Enhance an expert workforce to meet global cryptologic challenges* • Attract and leverage an expert and diverse workforce of mathematicians, computer scientists, engineers, signals analysts, intelligence analysts, language analysts, and staff to support the mission • Educate, train, and develop our workforce to sustain and strengthen our critical skills • Institute clear, uniform physical and personnel security practices and policies that allow us to work together, protect our nation's secrets, and enable aggressive counterintelligence activities • Recapitalize physical infrastructure to promote a modern, world class work environment that safeguards the health, safety, and quality of life of our employees	**Goal 4: Business Practices** *Create and integrate effective and efficient business management practices within the enterprise and with stakeholders* • Integrate budget and performance management to align investment decisions with corporate and national goals • Develop responsive corporate business processes which rapidly allocate and realign investments and programs in an integrated way • Strengthen foreign intelligence relationships and enhance domestic partnerships with government, industry, and academia to help us meet global cryptologic challenges

(U) Organization and Structure

(U) Organization charts for NSA/CSS as a whole and its Chief of Staff (where most support functions are located) appear below. The organizational structure is aligned to the Agency's mission and transformational imperatives. The heads of the Agency's mission, technology, research, and business management organizations report to the Agency Director, as do the Chief of Staff, General Counsel, and Inspector General. Two other direct reports – the Central Security Service (CSS) and the Joint Functional Component Command for Network Warfare – reflect the Agency's status as a combat support agency within DoD and the military/civilian synergy that is central to mission success.

(U) The organizational structure also reflects the multiple authorities of the Director NSA/Chief, CSS (DIRNSA). The DIRNSA serves in four different capacities simultaneously: Director of NSA (a Combat Support Agency under the Department of Defense); Commander, Central Security Service (overseeing the military Cryptologic system); Commander, Joint Functional Component Command, Network Warfare (as a component commander under United States Strategic Command); and Director, United States Security Service (as the federal government's executive agent for information assurance). In addition, the DIRNSA is senior member of the United States Intelligence Community and is the National SIGINT Manager.





(U) Principal Activities and Functions

(U//~~FOUO~~) A large, complex, high-technology enterprise with a worldwide presence, NSA/CSS performs a broad range of functions and activities – mission operations as well as support and governance functions – to accomplish its missions and prepare for the future. Following is a brief overview of the main categories of activities.

~~(S//SI//REL TO USA, FVEY)~~ SIGINT Mission Activities. Within the SIGINT mission, the principal activities consist of **acquiring** information, **understanding and interpreting** it, and **sharing it** with partners and customers who can act upon it.

(b)(1)
(b)(3)-P.L. 86-36

- *Acquiring information* includes determining how best to obtain information responsive to customers' intelligence needs, gaining access to that information, and capturing it. This in turn requires gaining a fundamental understanding of the world's many constantly-changing communications paths and technologies – [redacted] It also involves developing and fielding systems that capture signals and data and bring them into the cryptologic system.

- *Understanding and interpreting information* includes rendering raw data intelligible and determining its relevance, through techniques such as cryptanalysis, language analysis, and others; and then determining its meaning or significance by putting it in context, combining multiple

sources of information, determining patterns of activity, and other activities that turn signals and data into usable intelligence.

- *Sharing SIGINT information* includes delivering actionable intelligence information to customers and partners. This ranges from having embedded personnel give real-time intelligence to troops in harm's way, supporting our policymakers, diplomats and negotiators, passing threat information to our allies, or one of many other possible examples. The net effect is that NSA/CSS provides actionable intelligence where and when it is most needed, saving lives and advancing the goals and interests of the United States and its allies.

(U//~~FOUO~~) IA Mission Activities. The IA mission focuses on protecting classified and sensitive information and systems. Within the IA mission, NSA determines and responds to customer needs, assesses vulnerabilities, and develops architectures and solutions that enable secure and assured communications.

(U//~~FOUO~~) Network Warfare Enabling Mission Activities. The Joint Functional Component Command for Network Warfare (JFCC-NW) focuses on the optimization, planning, execution, and force management for the assigned missions of deterring attacks against the United States, its territories, possessions, and bases, and employing appropriate forces should deterrence fail, and the associated mission of integrating and coordinating DoD computer network attack (CNA) and computer network defense (CND) as directed by Headquarters.

(U//~~FOUO~~) Integrated Cross-Mission Activities. A significant portion of the NSA/CSS work is performed in four cross-cutting organizations, whose activities form an integral part of multiple missions:

- **(~~S//REL TO USA, FVEY~~) Mission Management.** The National Security Operations Center (NSOC) serves as NSA's mission management center. The NSOC provides worldwide situational awareness of NSA/CSS operations, and ensures that the system is focused the most important and current targets and challenges.

(b)(1)
(b)(3)-P.L. 86-36

- **(~~S//REL TO USA, FVEY~~) Network Threat Awareness.** The NSA/CSS Threat Operations Center (NTOC) provides a common operating picture of the global network and potential threats, supports the protection of classified and sensitive networks,

- ~~(S//REL)~~ **Commercial/Industrial Partnerships.** The NSA/CSS Commercial Solutions Center (NCSC) leverages industrial relationships and works with partners to address the strategic needs of NSA/CSS and the national security community

- (U//~~FOUO~~) **Foreign Relations.** NSA/CSS has highly productive relationships with counterpart organizations in foreign nations that support the conduct of both the SIGINT and IA missions. The Foreign Affairs Directorate manages these relationships, engaging with foreign partners in support of U.S. intelligence and national security.

(U//~~FOUO~~) Research and Development Activities. NSA must anticipate and keep pace with the rapid changes in technology that define and shape its mission environment. Accordingly, the Agency has extensive R&D activities that support its missions, discovering and developing the tools and techniques that will prepare the Agency for the future.

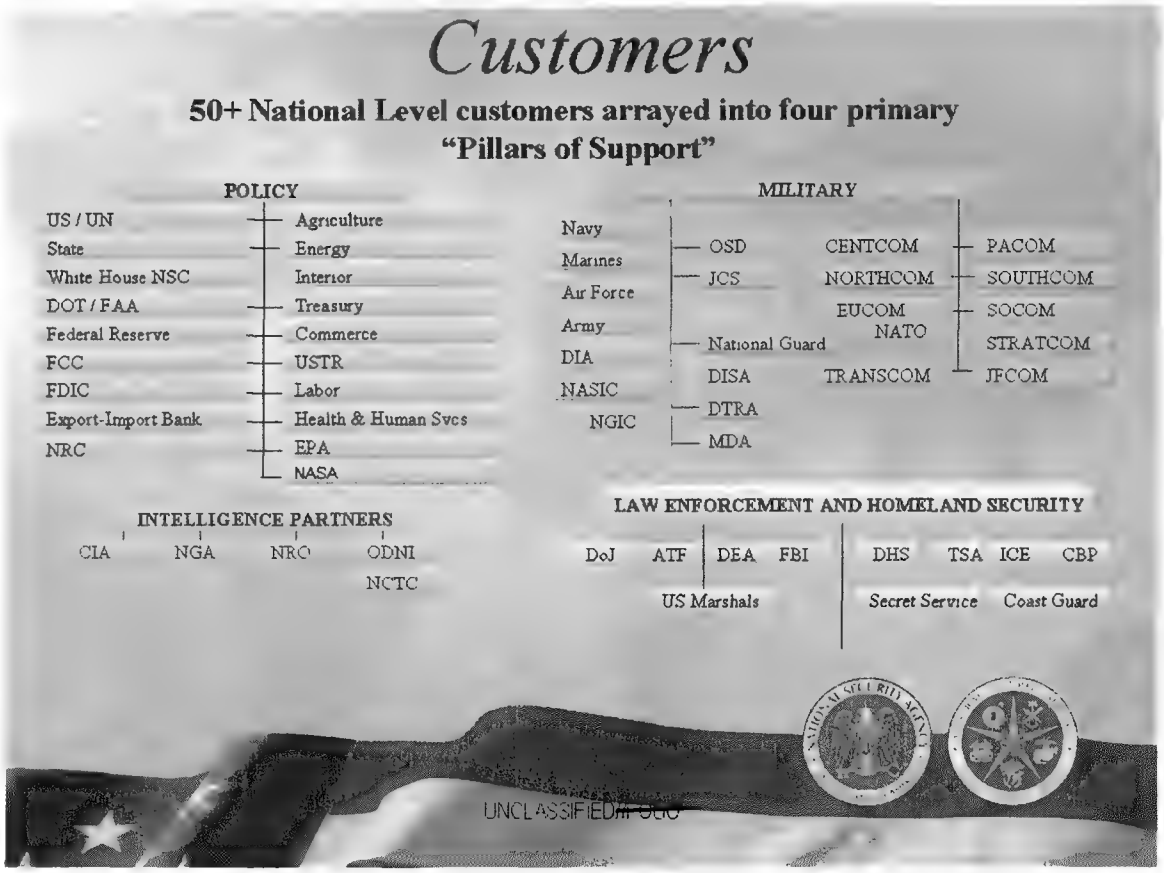
(U//~~FOUO~~) Information Technology Activities. NSA/CSS would not be able to carry out its mission with the development, engineering, implementation and maintenance of a resilient and robust IT infrastructure to store, process, and transmit and protect vast amounts of information at extremely high speeds. This work is the responsibility of the Technology Directorate, which was created within the past two years to spearhead and focus the Agency's program of rapid technology transformation .

(U//~~FOUO~~) Support and Governance Activities. Many other activities are required carry out NSA/CSS's mission and manage the enterprise that makes that mission possible. These include financial and acquisition management, human resources functions, education and training, security and counterintelligence, facilities and logistics, and many others, as well as processes to support the effective operation of the senior leadership and governance functions. Many of these functions reside in the NSA Chief of Staff structure, and others in the Business Management Integration organization. An essential element in the Agency's work is the array of activities, from our General Counsel and Inspector General structures, through training, reporting, auditing, and other work across the Agency aimed at ensuring strict adherence to all laws, regulations, policies and other applicable authorities, especially those relating the rights of U.S. persons.

(U) Customers, Partners, Role in the Community

(U) *Customers*

(U//~~FOUO~~) The NSA/CSS SIGINT and IA missions serve many customers within the U.S. Government. SIGINT customers are listed on the chart below. They include numerous organizations and commands within the Department of Defense, elements of the Office of the Director of National Intelligence and other intelligence agencies, and the full spectrum of civilian agencies and departments. Many of these customer organizations also serve as partners in the conduct our SIGINT mission. NSA/CSS also provides Information Assurance products and services to many of these same customers.



(U) *Partners*

(U//FOUO) **Government.** NSA/CSS maintains robust and productive partnerships. These yield mission results beyond what any individual agency could achieve alone. Several primary partnerships are with CIA, NGA, NRO, and FBI, with major areas as follows: (b)(1) (b)(3)-P.L. 86-36

- (U//~~FOUO~~) NSA maintains a strong partnership with FBI for the benefit of both organizations. NSA reports foreign intelligence as a result of its SIGINT collection, processing and analysis in response to FBI formal requirements, which enables FBI to better perform its mission. FBI leverages NSA's extensive subject matter expert base and tremendous technical expertise, by requesting technical assistance to support FBI's law enforcement mission. In return, NSA benefits from information sharing from FBI activities.

(b)(3)-P.L. 86-36

- (~~S//REL TO USA, FVEY~~) **Foreign Relations.** NSA/CSS maintains foreign partnerships that

- (U//~~FOUO~~) **Academia.** NSA/CSS has an array of relationships with academia that advance its SIGINT and IA missions. These arrangements leverage academic expertise against current mission accomplishment, strengthen our educational institutions, and help build the talent pool in fields – such as mathematics, computer science, advanced engineering and languages – vital to the Nation in general and the Intelligence Community in particular.

(b)(1)
(b)(3)-P.L. 86-36

(U) Role in the Community

(U//~~FOUO~~) The role of NSA/CSS in the Intelligence Community takes multiple forms, driven by several factors that make the Agency unique: the nature of SIGINT; the particular accesses, analytic, and technical capabilities of NSA/CSS; the synergy between the multiple missions that NSA/CSS is charged with; and the combination of authorities delegated to the DIRNSA, which in some instances carry beyond the organizational boundaries of NSA/CSS and into the broader Intelligence Community at large. These factors can be summarized as follows:

- **Unique Nature of SIGINT.** SIGINT is a unique form of intelligence – it has been said that SIGINT is like "putting your head in the other team's huddle." SIGINT provides information

(b)(3)-P.L. 86-36

available through no other source, and at its most successful, SIGINT obtains the secrets that foreign adversaries and rivals are trying hardest to protect.

- **Unique Enterprise.** The reason NSA/CSS can provide SIGINT is because of the remarkable capacities of the Agency - The SIGINT mission cannot be effectively performed without bringing all these factors to bear.

- **Unique Synergy of Missions.** In addition the authority and capability to conduct the SIGINT mission, the combination of missions – SIGINT and IA, military and civilian – are mutually reinforcing. Work in each of these areas - strengthens mission performance in the others. Expertise and capabilities in both areas is essential in providing security in cyberspace and enabling network warfare.

- **Unique Authorities.** The DIRNSA has authorities that run beyond the organizational boundaries of NSA/CSS. The DIRNSA's authorities extend into the military departments and DoD agencies, and, as National SIGINT manager, across the Intelligence Community.

(U//~~FOUO~~) This combination of factors makes NSA/CSS an effective member of the IC in many ways. The Agency is a contributor of intelligence that is valuable in its own right and when fused with other sources; a partner enabling other IC agencies to better achieve their mission objectives; a major factor in contributing to the success of ODNI-level intelligence production; and a force for integration across the IC. More broadly, NSA/CSS participates actively in ODNI-level functions and activities, from the DIRNSA's membership on the DNI's Executive Committee, through alignment with the ODNI's strategic plans and objectives, membership on boards and panels, exchange of personnel with other IC agencies, participation in the ODNI program and budget process, and other work too extensive and varied to detail here.

(U) Conclusion

(U//~~FOUO~~) NSA/CSS is an integral and essential member of the Intelligence and Defense communities, and its work contributes greatly to the mission success of its many customers. The Agency's work helps save lives, advance U.S. goals and alliances, defend vital networks, and protect American rights and liberties. The men and women of NSA/CSS come to work every day to defend the Nation and secure its future.

PROVIDING AND PROTECTING VITAL INFORMATION FOR OUR NATION

The National Security Agency (NSA) has served the people of the United States as the Nation's codemakers and codebreakers for over fifty years. In this role as the "Cryptologists for the Nation," the men and women of NSA have helped to secure the Nation's communications while at the same time exploiting the communications of our foreign adversaries.

Today, the mission of NSA and its military component, the Central Security Service (CSS), has transformed to meet the challenges and opportunities of the information age. Codebreaking has evolved into a comprehensive Signals Intelligence system that spans the globe, gathering critical foreign intelligence from our adversaries' communications and networks. The Signals Intelligence mission provides senior decision-makers and deployed warfighters in the field with the information that gives them a decisive edge over our adversaries.

In a similar manner, codemaking has transformed into Information Assurance, which not only secures communications in-transit, but also provides computer and network security capabilities for information as it is being processed and stored. The Information Assurance mission protects critical communications on national security systems, from the foxhole to the White House, enabling warfighters and decision-makers to communicate securely anywhere in the world in real time. Under National Security Directive 42, the Director of NSA is responsible for the protection of national security systems within the federal government.

The NSA/CSS mission is focused on saving lives, defending vital networks, and advancing U.S. goals and alliances – while at the same time protecting the privacy rights of U.S. persons. NSA/CSS is uniquely positioned to accomplish its mission through the exceptional skills of its workforce. Here at NSA/CSS, our teams of mathematicians, computer scientists, language analysts, intelligence analysts, engineers, and a host of others in supporting roles, solve some of the most vexing intelligence challenges that face the Nation.

As the information age continues to transform the world, NSA/CSS will continue to transform its approach to its mission. The men and women of NSA/CSS will keep pace with these changes, even as the Signals Intelligence and Information Assurance missions evolve into the realm of Computer Network Operations. We will face these challenges as we have for the last half century – with determination, creativity, and a singular focus on what has always been the bottom line: the safety and security of our Nation. ■

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

Defending Our Nation. Securing The Future.

SAVING LIVES

Today's world poses a wide range of threats to the safety and security of the United States and our allies. Global terrorism puts at risk the lives of our citizens at home and abroad, as well as the U.S. and allied forces engaged in countering this challenge. Other threats stem from economic, environmental, health, and other conditions around the world that our Nation is committed to help address. Working with our partners in the Defense and Intelligence Communities, NSA/CSS provides direct support as our Government works to protect the lives and safety of our citizens and comes to the aid of others.

Saving Lives – The Foundation of NSA/CSS

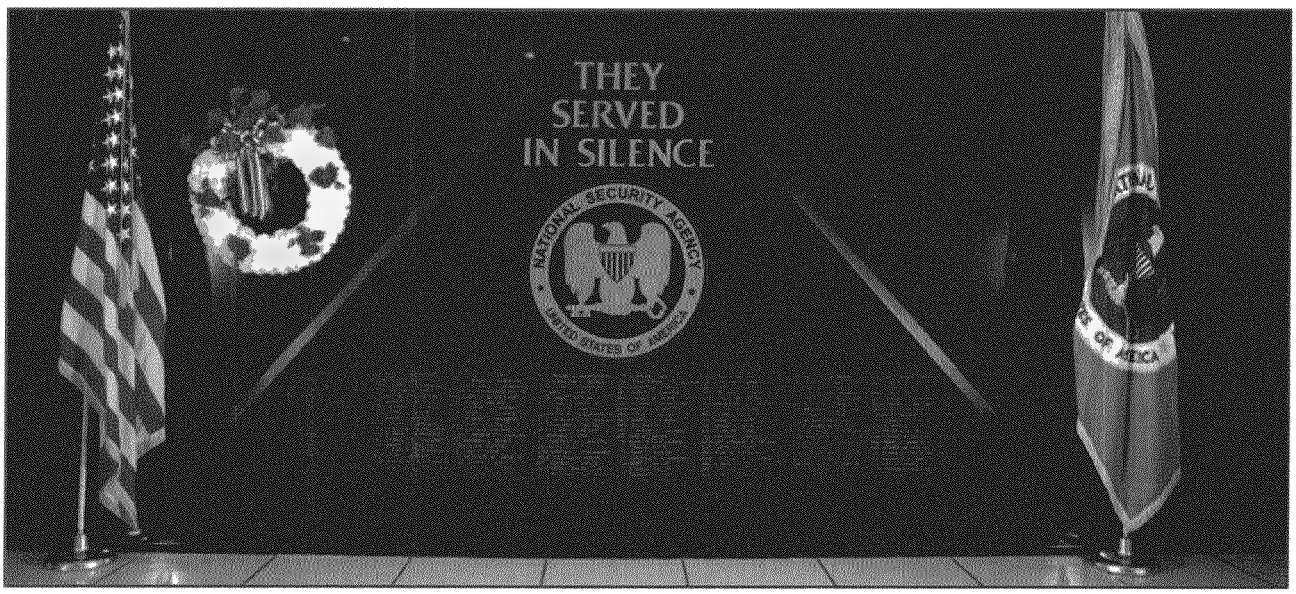
Saving lives has historically been at the heart of the cryptologic mission. During WWII, Signals Intelligence helped defeat the German U-boats in the North Atlantic and win the Battle of Midway in the Pacific. These successes hastened Allied victory and the end of the conflict.

NSA/CSS was established in response to the lessons learned from WWII. Initially focused on meeting the challenges of the Cold War, NSA/CSS has evolved and continues to transform in the face of an ever-changing global environment. Through its dual mission to provide and protect vital national security information, today's NSA/CSS is committed to protecting the lives of our citizens at home and abroad, warning of impending threats to our Nation and its allies, supporting our troops in harm's way, and protecting our national leaders as they travel into hostile regions. This commitment – keeping our Nation and its allies safe – is central to the everyday activities of the men and women of NSA/CSS.

Combating Terrorism

In today's fight against terrorism, NSA/CSS's role is vital. Instead of large, powerful nation-states, terrorist adversaries are loose-knit, dispersed groups, blending readily into civil society. Fighting this enemy starts with the challenge of finding him.

The mission, skills, and technology of NSA/CSS are uniquely suited to this challenge. Terrorist groups rely on modern computing technology and the global communications network to recruit, plan, and act. Signals Intelligence collection and analysis can reveal terrorist locations and intentions, while Information Assurance helps keep our own and our partners' most important communications secure against enemy exploitation.



Signals Intelligence has served as an essential tool in finding, fighting, and capturing terrorists in Iraq, Afghanistan and elsewhere around the world. In one of many examples, NSA/CSS was a key contributor to multi-agency efforts leading to the elimination of Al Qaida in Iraq leader Abu Musab al-Zarqawi.

Recent advances in technology have made NSA/CSS's support more important – and more valuable – than ever. Information on quick-moving and agile terrorist operations is often highly perishable. Fast action is essential. When information on a terrorist's location or plans can be relayed quickly to troops on the ground, lives can be saved. Conversely, delay can prove fatal. NSA/CSS has developed and now employs a technology that allows us to deliver actionable intelligence to allied troops within minutes of discovery. This new technology has been hailed by our commanders in the field as an extremely effective tool that has contributed to a significant increase in the effectiveness of combat operations.

Saving lives has also been the focus of our work to protect against improvised explosive devices (IEDs). Inexpensive, easy to build, and deadly, these devices can be planted along a roadside or carried by a vehicle or suicide bomber. NSA/CSS and other community partners are working towards countering these weapons.

Hundreds of our personnel literally serve side-by-side with our troops in combat, risking their lives and safety to protect our freedoms. A somber, deeply affecting tribute to their work is the Memorial Wall at NSA/CSS Headquarters at Fort Meade, Maryland. Bearing the phrase "They Served In Silence," it commemorates the sacrifices of those NSA/CSS personnel who have given their lives for our Nation.

Protection at Home and Abroad

The past several years have seen the United States "take the fight to the enemy" by actively combating terrorism abroad. At the same time, NSA/CSS works with our partners and counterparts to discover and warn of threats stemming from overseas that would strike here at home. We provide information gleaned from foreign intelligence collection to the FBI, and intelligence information and Information Assurance support to the Department of Homeland Security and other agencies that are responsible for ensuring domestic safety.

On many occasions, NSA/CSS information has assisted partners in investigating extremist threats, making arrests, and successfully prosecuting those wishing to do harm to Americans at home.

NSA/CSS also provides indications and warning of impending terrorist attacks or operational planning abroad. Working as part of the Intelligence Community, we provide timely and vital information to senior decision-makers, enabling them to take appropriate actions to protect U.S. personnel and interests overseas.

As a special focus, NSA/CSS personnel support foreign travel by high-level U.S. Government officials, ensuring that the appropriate U.S. agencies are aware of any real or perceived threats against those officials.

Supporting Humanitarian and Peacekeeping Efforts

NSA/CSS also provides relief operations in hostile areas with intelligence, communications networks, and communications security support. U.S. and international peacekeeping forces receive real-time updates, enabling them to preempt and defuse potential problems, resulting in lives being saved and the promotion of peace. ■

National Security Agency/Central Security Service

Defending Our Nation. Securing The Future.

Saving Lives

(b)(3)-P.L. 86-36

Key Advancements in Signals Intelligence Support: The Real Time Regional Gateway

~~*(S//SI//REL TO USA, FVEY)*~~ *NSA/CSS has implemented a "right people, right methods, and right capabilities" approach for* [redacted] *especially in Iraq and Afghanistan.*

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

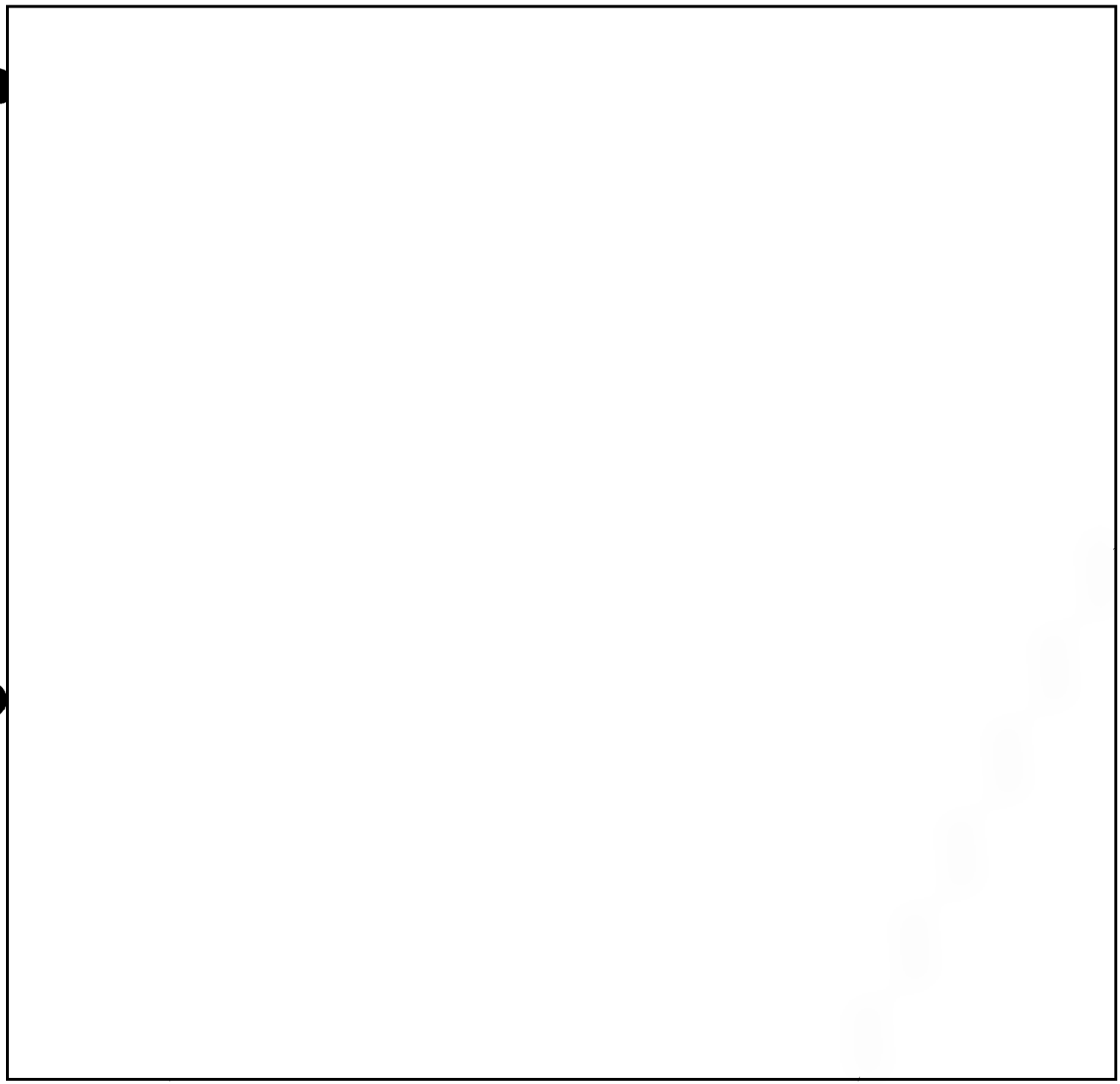
~~(C)~~ The hallmark of this approach is the high degree of collaboration between NSA/CSS and our IC customers and partners including the Services.

(i)

~~(S//SI//REL TO USA, FVEY)~~ These analysts are using the Real Time Regional Gateway (RT-RG), a revolutionary Signals Intelligence architecture

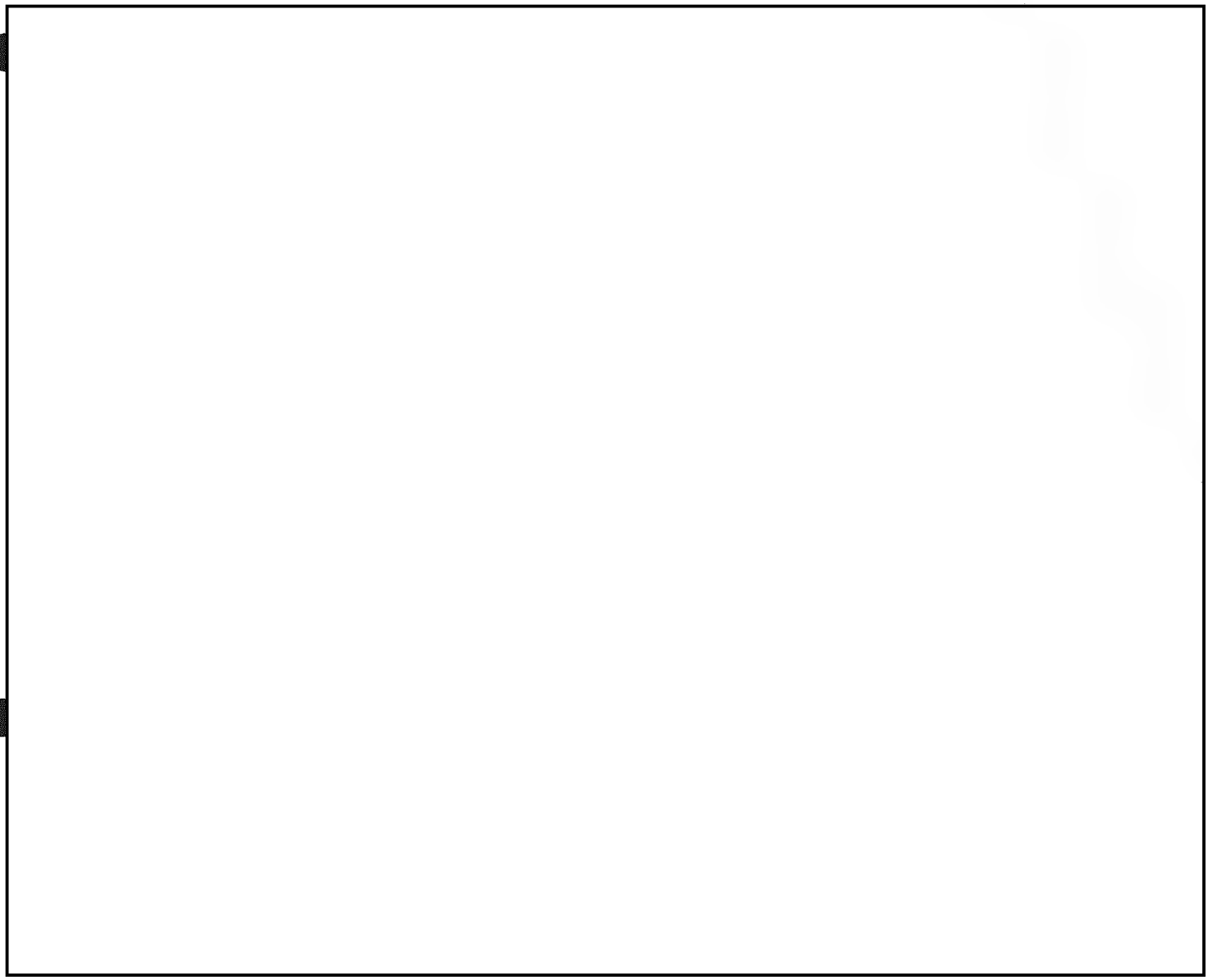
The RT-RG program is bringing the full Signals Intelligence analysis, processing, and exploitation power of NSA/CSS to deployed U.S. and government agencies and military forces along with our 2nd and 3rd party partners in Theater through special agreements.

RT-RG provides Signals Intelligence analysts near real-time access to



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36



National Security Agency/Central Security Service

Defending Our Nation. Securing The Future.

Saving Lives

SIGINT Contributions to Countering Terrorism

(U//~~FOUO~~) NSA/CSS applies unmatched cryptologic capability against a multitude of terrorist communications. Our success enables effective operations and decision making by U.S. and foreign military, law enforcement, and intelligence services to locate and neutralize threats to the Nation, at home and abroad, in support of the Global War on Terrorism.

The Challenge Facing the Nation

(U//~~FOUO~~) Terrorists threaten U.S. and foreign partner interests at home and abroad, using violence to influence political, financial, and military decisions. Sunni Islamic extremists, especially visible since the 9/11 attacks, also seek to influence cultural and religious outcomes. Terrorists kill people and destroy infrastructure – ideally with maximum publicity – primarily by attacking soft targets in government, transportation, and commercial sectors. Military, police, and security personnel in non-hardened situations are also attractive targets. Weapons of choice include suicide bombers and improvised explosive devices.

The Nation's Strategy

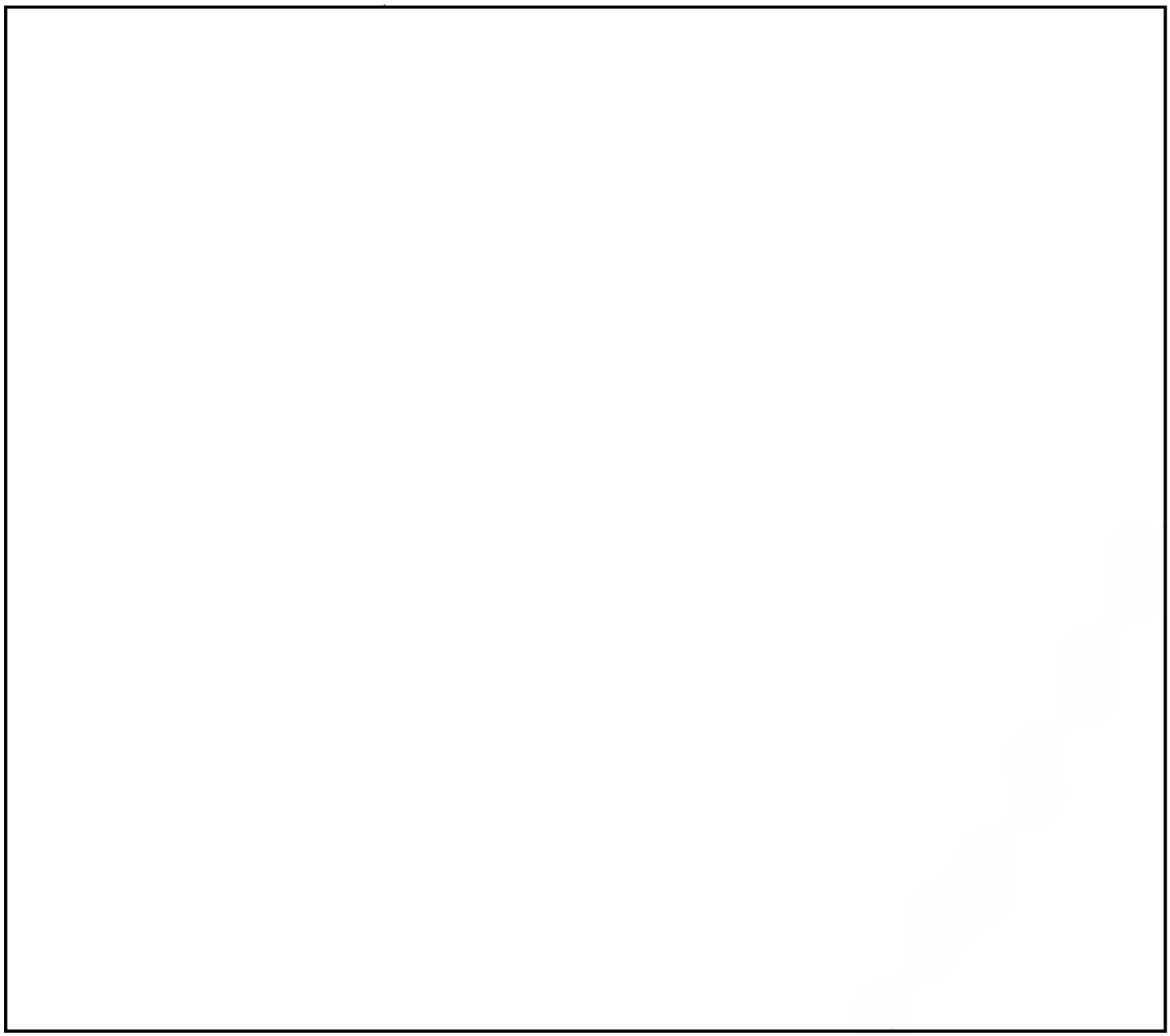
(U//~~FOUO~~) The U.S. Government (USG) counterterrorism response must include a mixture of soft and hard as well as offensive and defensive initiatives such as:

- extensive intelligence gathering and effective sharing, both within USG circles and with our foreign partners;
- disruption of terrorist command and control, communications, recruiting, training, facilitation, finance, travel, and operational planning capabilities;
- a full range of security inspection, interdiction, and disruption activities at or before the borders; and
- both defensive and targeted offensive military action.

How NSA/CSS Contributes

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

National Security Agency/Central Security Service

Defending Our Nation. Securing The Future.

Saving Lives

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Military Intelligence Support

(b)(3)-P.L. 86-36

~~*(S//REL TO USA, FVEY)*~~ *Meeting the demand for global, timely, and actionable intelligence requires a strong partnership between NSA/CSS and the U.S. Military Services. This partnership allows seamless, collaborative execution of the full spectrum of SIGINT.*

The Challenge Facing NSA/CSS

(U//~~FOUO~~) NSA/CSS faces a number of challenges in sustaining its mission in the 21st Century. The target access and exploitation environment is vastly more complicated than it was a decade ago. The volume of data in the global information environment grows daily, making it more difficult to isolate the information that our customers need. The rapid changes in technologies and ever-increasing variety of communications challenge our ability to keep pace with the target environment. Increased commercial availability of encryption and other security methods make it difficult to quickly access the intelligence value. To meet these challenges, NSA/CSS has developed new business practices to extract information, manage data, correlate information derived from multiple sources, and provide the resulting intelligence to the customer community.

NSA/CSS's Strategy

This re-alignment is the result of a joint US Under-Secretary of Defense for Intelligence

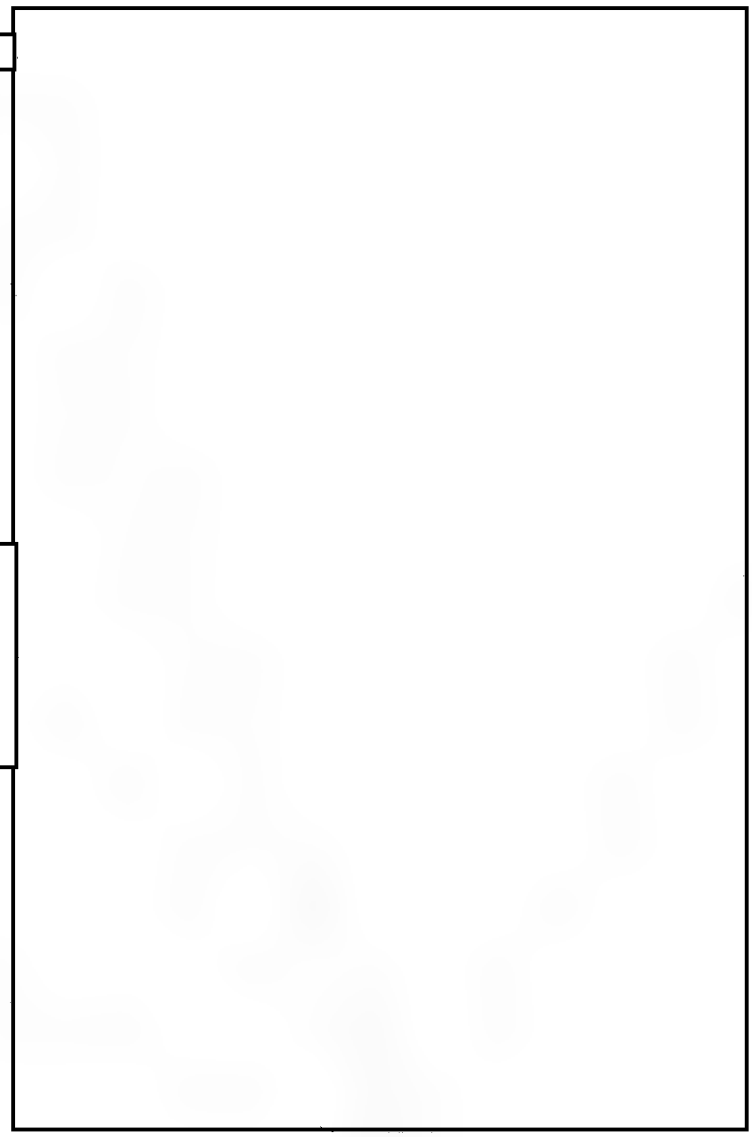
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

and NSA/CSS effort to best capture the joint nature of Cryptologic operations.

How NSA/CSS Contributes

(~~S//REL TO USA, FVEY~~) our successes in current operations (the Global War on Terrorism, Operations ENDURING FREEDOM and IRAQI FREEDOM) continue to guide our efforts toward providing vital intelligence at all levels of command. At the tactical level, the sharing of SIGINT data enriched with SIGINT-related IMINT, HUMINT, MASINT, and open source data is facilitated with stronger analytic tools and regionally relevant data repositories providing a comprehensive and readily accessible view of the battlespace.

in order to facilitate the streaming of complete, cohesive, timely, and actionable intelligence into the tactical commander's decision space. At the operational level, the Joint Intelligence Operations Centers and increasingly integrated tactical assets within the Cryptologic Centers will build and strengthen the role of the COCOMs within the Cryptologic Enterprise and eliminate the technical and doctrinal barriers that hinder effective, synchronized operations across the Service and Intelligence Communities.



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

National Security Agency/Central Security Service

Defending Our Nation. Securing The Future.

Saving Lives

Countering Improvised Explosive Devices

~~*(S//REL TO US, FVEY)*~~ *Improvised Explosive Devices (IEDs) currently represent the greatest threat to Coalition forces, and by extension to U.S. and Allied forces, around the globe. These devices can be planted along a roadside or carried by a vehicle or suicide bomber. NSA/CSS and other Intelligence Community partners have undertaken a broad array of initiatives to defeat this inexpensive terrorist weapon which is so easy to construct and deploy.*

[redacted] b)(3)-P.L. 86-36

The Challenge Facing the Nation

(U~~//FOUO)~~ Nearly every day in the news, there are stories about explosions that injured or killed Coalition troops or Iraqi civilians. These IEDs have had a devastating effect, not only on the morale of Coalition troops, but also on that of the Iraqi population, most of whom are innocent victims of this weapon.

(b)(1)
(b)(3)-P.L. 86-36

The Nation's Strategy

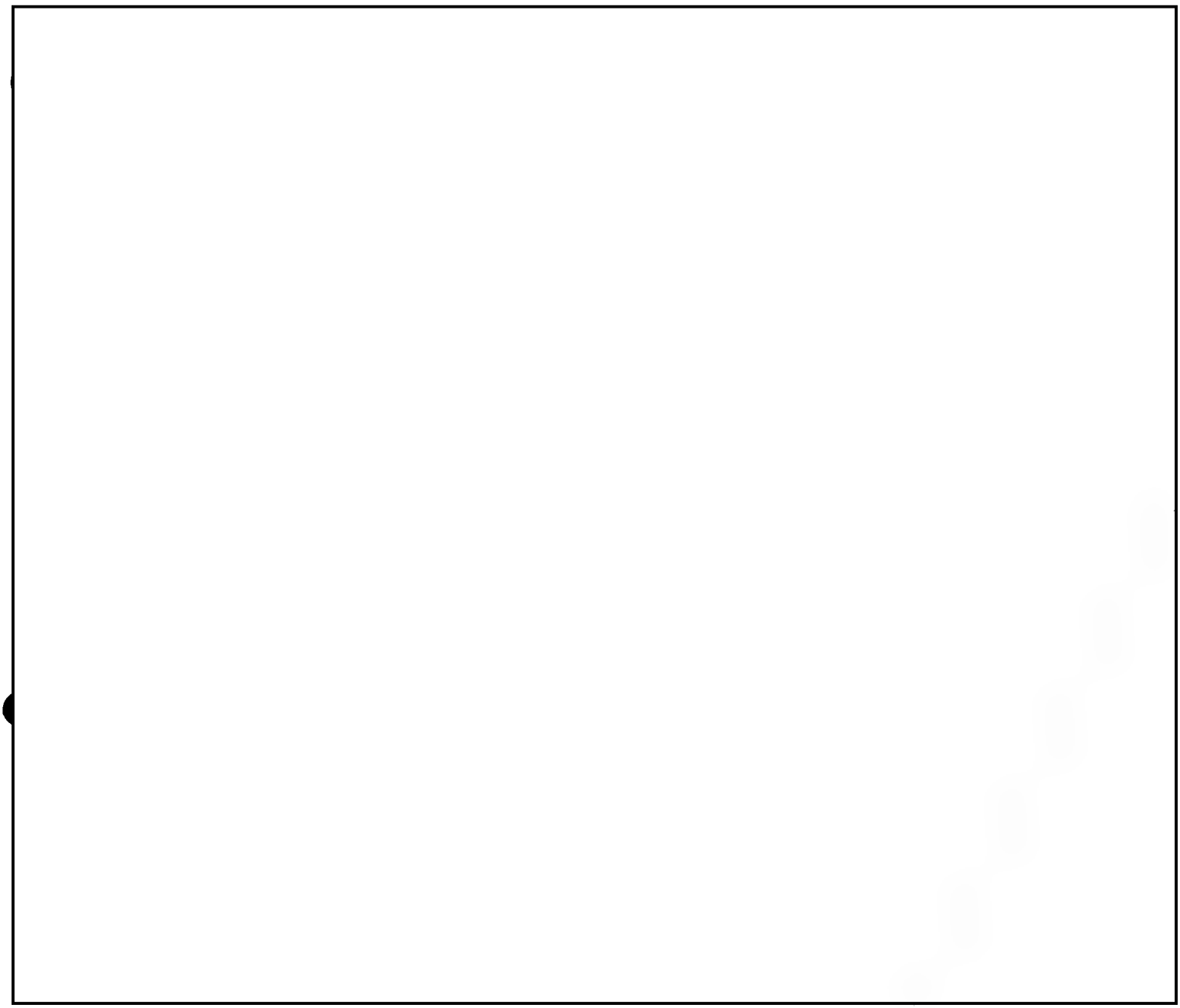
~~(S//SI//REL TO US, FVEY)~~

[redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

National Security Agency/Central Security Service

Defending Our Nation. Securing The Future.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Saving Lives

Protecting U.S. Citizens Abroad

(U//~~FOUO~~) The Nation has no higher duty than protecting the lives of its citizens against foreign threats. Our people face dangers and risks when they are abroad. NSA/CSS uses all its resources in support of national efforts to ensure their safety.

The Challenge Facing the Nation

(U//~~FOUO~~) As described in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), U.S. responsibilities to protect the lives of its citizens does not end at the border. For example,

In each situation, the U.S. evaluates specific criteria to assess the potential threat and design an appropriate security and intelligence support structure in response.

(b)(3)-P.L. 86-36

The Nation's Strategy

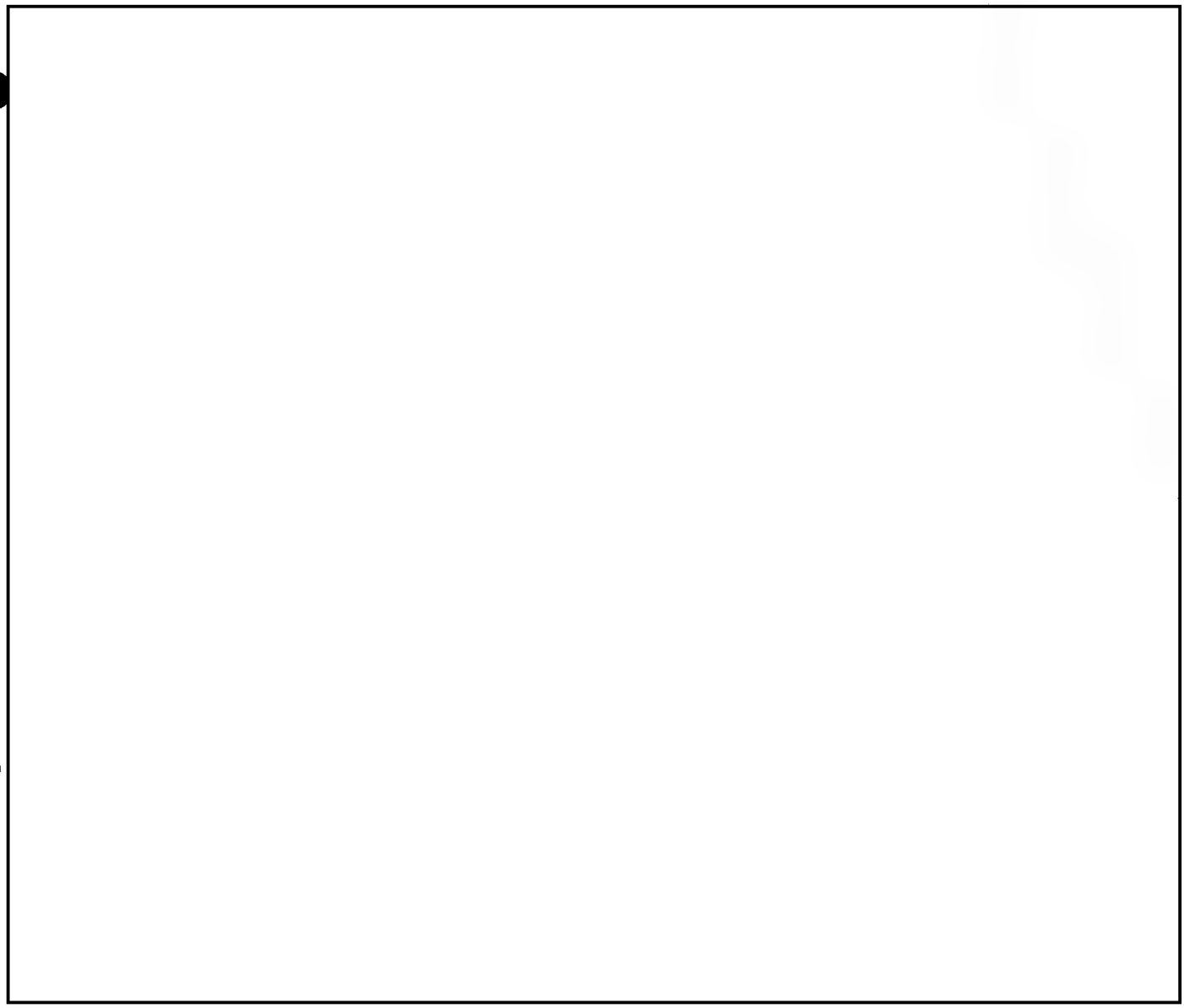
(U//~~FOUO~~)

Also, when high-ranking U.S. officials travel abroad, primary responsibility for their well being falls in the hands of the U.S. Secret Service (USSS).

How NSA/CSS Contributes

~~(S//REL TO USA, FVEY)~~ NSA/CSS has significantly improved close, secure collaboration among U.S. Government and intelligence community (IC) partners in line with IRTPA goals to protect U.S. lives and interests

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



DEFENDING VITAL NETWORKS

Vital national security information, as well as the networks and systems on which it resides, are under near-constant exploitation by adversaries from around the world. NSA/CSS has the expertise and technology uniquely suited to address this problem, and a long history of providing security for national security systems. Insights and information gained from the Signals Intelligence mission, combined with the expertise and capabilities offered by the Information Assurance mission, make NSA/CSS a key player in defending vital networks against the threats of the Internet age.

The Threat

Cyberspace – the equipment, communications infrastructure, and software that constitute today's global information network – has become the virtual central nervous system of the world's commercial, economic, social, governmental and military activity. The U.S. has reaped the benefits of cyberspace – and depends upon cyberspace – as fully as any other nation, if not more so. Yet for all its benefits, cyberspace is fraught with risk.

Modern networks and applications are often convenient and easy to use, but vulnerable to intrusion and attack. As a result, foreign adversaries and criminals at home and abroad can readily steal, change, or destroy information or control, damage, or shut down networked systems that are essential to the economy, government at all levels, and military operations.

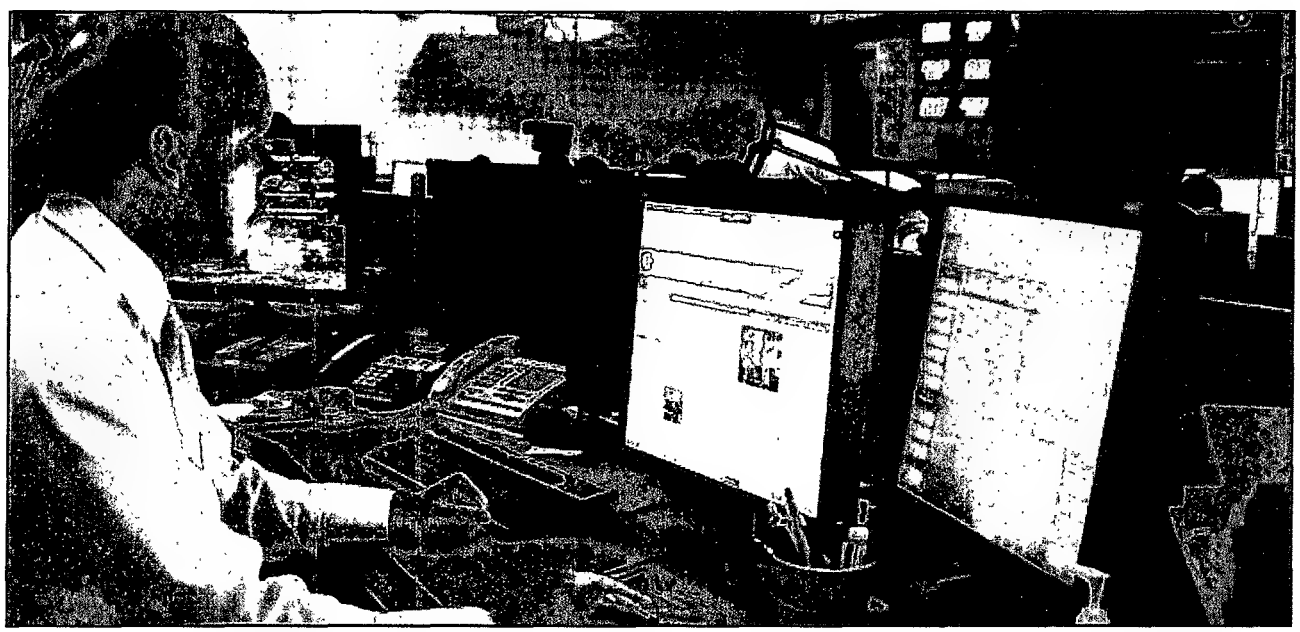
Threats to national security systems can jeopardize the Government's ability to defend the Nation and perform other fundamental functions. By Presidential Directive, the Director of NSA is designated as the National Manager for the security of national security systems across the federal government.

The Elements of Defense

What does it take to defend against this growing threat? Security in this arena means understanding what is being attacked, understanding the foreign threats, and understanding the tools and practices that can strengthen network security. NSA/CSS brings all these to the table.

Situational Awareness

Through its Threat Operations Center, NSA/CSS monitors



potential threats to Defense Department systems. This center is staffed by analysts, engineers, and computer scientists drawn from across the federal government. Using the best commercial and government-developed tools, and drawing on Signals Intelligence expertise from NSA/CSS and its allies and partners across the Government, these experts track threats to the security of DoD networks. The expertise of our workforce – mathematics, cryptanalysis, engineering, and computer science – is instrumental in addressing the expanding challenges of cyberspace.

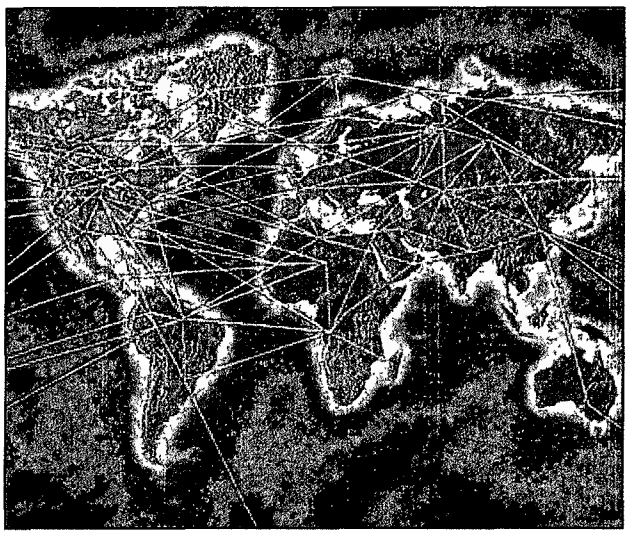
Discovering Vulnerabilities

NSA/CSS improves the security of our Nation's critical national security information by helping our customers identify and correct vulnerabilities in technology and operations that could be used to compromise the security of the information. We lead the Nation in providing evaluation and guidance in the security disciplines that identify and mitigate these vulnerabilities. This guidance is provided directly to our customers, including the departments of Defense, State, Treasury, Justice, and Homeland Security, enhancing the security posture of their critical networks.

Cryptographic Solutions

NSA/CSS is the U.S. Government's sole provider of encryption technology for the protection of highly classified information. We accomplish this through a unique combination of mathematics and engineering disciplines. NSA/CSS develops encryption algorithms, certifies their implementation into national security systems, and evaluates their performance over their lifecycle. This ensures that the critical information required by our Nation's decision-makers is protected from exploitation by adversaries.

Not only does NSA/CSS provide strong encryption to the U.S. Government, it also provides a state-of-the-art national security infrastructure to support these encryption products. NSA/CSS is developing an automated system for delivering and updating security capabilities that will be far faster, more efficient, and more comprehensive than current methods.



Technical Expertise

We also assist other federal agencies in keeping their information systems secure. NSA/CSS helps develop design security standards for information technology products. Industrial vendors of information systems design their products to meet these standards and then submit them to accredited test labs for validation that the standards are met.

NSA/CSS also provides key customers with engineering expertise covering a wide range of technical disciplines. Our subject matter experts work closely with customers to ensure that systems under development include the security features necessary to defend vital networks.

Looking Ahead

We will continue to pursue these critical capabilities. NSA/CSS is a partner in the Comprehensive National Cybersecurity Initiative, along with the Department of Homeland Security and over twenty other federal departments and agencies. We are providing technical expertise and technology to support the successful implementation of a frontline defense for critical federal information systems. As the issue of cyber-security intensifies in importance across the federal government, and the capabilities of our adversaries continue to advance, NSA/CSS will continue to play a leadership role in defending the Nation's vital networks. ■

Defending Vital Networks

Comprehensive National Cybersecurity Initiative (CNCI)

(U//~~FOUO~~) It is often said that the best defense is a good offense. The CNCI applies that strategy to the cyber domain. The CNCI seeks to address current cybersecurity threats and anticipate future threats and technologies in order to prevent, deter, and protect the U.S. Federal government (.gov) domain against cyber intrusions. The strategy includes establishing shared situational awareness across the federal government.

The Challenge Facing the Nation

~~(S//REL TO USA, FVEY~~) The explosive growth of the Internet has sparked tremendous growth in information exchange and efficiency in only a generation and changed the way the world communicates and does business. The effect of the Internet on everyday life is unmistakable. Modern communications and information systems have become the virtual nervous system of society at large. Increasingly, these critical systems are vulnerable to intrusion, theft, destruction, and corruption. This threat to society goes to the core infrastructure of the nation.

The Nation's Strategy

(U//~~FOUO~~) On January 8, 2008, the President signed an order establishing a plan to increase U.S. security in cyberspace. That plan included greatly improving the security of governmental systems; creating a clear picture of threatening or malicious activity; and describing and assigning responsibilities to various organizations throughout the federal government.

How NSA/CSS Contributes

[redacted]

[redacted] The capabilities that NSA/CSS brings to the CNCI will not only help provide an integrated defense against foreign computer network operations against the U.S., but will also provide decision-makers with options for how to mitigate those threats.

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

[redacted] The CNCI seeks to detect and deter cyber attacks against government systems. We will contribute our capabilities and expertise to:

- Provide advanced indications and warnings of foreign-based malicious cyber attacks against the U.S.

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

(U//~~FOUO~~) NSA/CSS will also provide authorized technical assistance to the Departments of Homeland Security and Defense, as well as the Law Enforcement community, to help their domestic cybersecurity efforts. Such collaboration, within existing authorities, will ensure that the government is poised to effectively, efficiently, and transparently take advantage of the expertise throughout the community to address the threat to cyberspace security.

Examples/Stories (b)(1) (b)(3)-P.L. 86-36

(U//~~FOUO~~) Due to the unprecedented unity of effort assembled across the broad federal coalition of participating departments and agencies, the National Cyber Study Group (NCSG), with NSA/CSS participation, has successfully accomplished several major activities:

- (U) Completed a human resource strategy for hiring, training, and retaining robust cybersecurity workforce. (b)(3)-P.L. 86-36

(U//~~FOUO~~) The above activities have provided a foundation for NSA/CSS to gain momentum for long-term success.

National Security Agency/Central Security Service

Defending Our Nation. Securing The Future.

Defending Vital Networks

Maintaining Situational Awareness of Threats to Critical Federal Networks

(U//~~FOUO~~) Our national security and economic well-being depend on our Nation's ability to successfully move information over protected, networked information systems. NSA/CSS stands ready to detect and deter cyber threats and to defend critical national information networks

(b)(1)
(b)(3)-P.L. 86-36

The Challenge Facing the Nation

(U) The networks and systems that currently comprise our nation's cyber "nervous system" are based on a commercial architecture developed with an eye to interoperability and growth rather than security. Over the past fifteen years, as these systems became an essential part of day-to-day government, military, and economic activity, the abilities of hostile actors to compromise and exploit these vital networks have outpaced our ability to defend them.

~~(S//REL TO USA, FVEY)~~ When a network is compromised, information can be stolen, changed, or destroyed. Worse, the systems themselves can be controlled, damaged, or even shut down.

The Nation's Strategy

~~(S// REL TO USA, FVEY)~~ Since May 2007, 20+ departments and agencies have participated in formulating a new national strategy to defend our networks: the Comprehensive National Cybersecurity Initiative (CNCI), approved by the President on 8 January 2008 (summarized in its own issue paper). The CNCI harnesses the power of intelligence collection and analysis across all federal agencies to provide awareness, understanding, and early warning of cyber threats to our critical networks.

How NSA Contributes

~~(S// REL TO USA, FVEY)~~ As the U.S. government's largest repository of expertise

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

in exploiting and protecting networks, NSA/CSS is uniquely positioned to support the national strategy. We are the Intelligence Community's leading provider of cyber threat information; we make daily strides in our abilities to detect and mitigate cyber intrusions and engage in a number of analytic activities.

- *Threat analysis* provides a comprehensive understanding of the intentions, capabilities, and activities of the adversary. It also uncovers current and emerging technologies, capabilities, and systems that could be used to attack or exploit systems owned by or of interest to the U.S. and its allies.
- *Activity analysis* allows for the discovery of unknown, significant intrusion activity, in-depth analysis of known intrusion sets, and trend analysis.
- *Network analysis and cyber target development efforts* monitor, characterize, and report on foreign digital networks, organizations, and personas in cyberspace and target development to gain actionable intelligence on cyber adversaries.

~~(S// REL TO USA, FVEY)~~ To help us achieve success, NSA/CSS has placed a strong emphasis on building cyber partnerships throughout the U.S. government and with private industry and our allies. Government partners include the Federal Bureau of Investigation/Department of Justice, National Cyber Investigative Joint Task Force, and Department of Homeland Security/U.S. Computer Emergency Readiness Team. Industry partners include the Defense Industrial Base, a group of selected, cleared defense contractors.

~~(TS//SI//REL TO USA, FVEY)~~

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

National Security Agency/Central Security Service
Defending Our Nation. Securing The Future.

Defending Vital Networks

Joint Communications Security (COMSEC) Monitoring Activity (JCMA): Support to U.S. Forces Conducting Operations in Harm's Way

(U//~~FOUO~~) JCMA, a joint-service, Joint Staff-sponsored activity of NSA's Information Assurance Directorate, is composed of a Headquarters Operations Center, located at NSA/CSS Headquarters, and six Regional COMSEC Monitoring Centers located throughout the world.

The Challenge Facing the Nation

~~(C//REL TO USA, FVEY)~~ Adversarial knowledge of military operations could put missions and lives at risk. For this reason, U.S. government entities request that JCMA monitor their unclassified communications to identify information that adversaries could exploit; JCMA also provides advice to mitigate risks. Results of COMSEC monitoring assist in force protection and also provide indications of what an adversary could learn about U.S. operations. JCMA is currently providing operational force protection support

The Nation's Strategy

(b)(3)-P.L. 86-36

~~(S//REL TO USA, FVEY)~~ The Information Assurance Directorate's core mission is to improve the security of critical operations and information by providing know-how and technology to its customers when they need it. JCMA's customers are helping to keep our nation safe by having their security posture evaluated and taking decisive action when they receive results. As each command addresses vulnerabilities in their COMSEC, it makes the enemy's job that much harder and helps make the country more secure.

How NSA Contributes

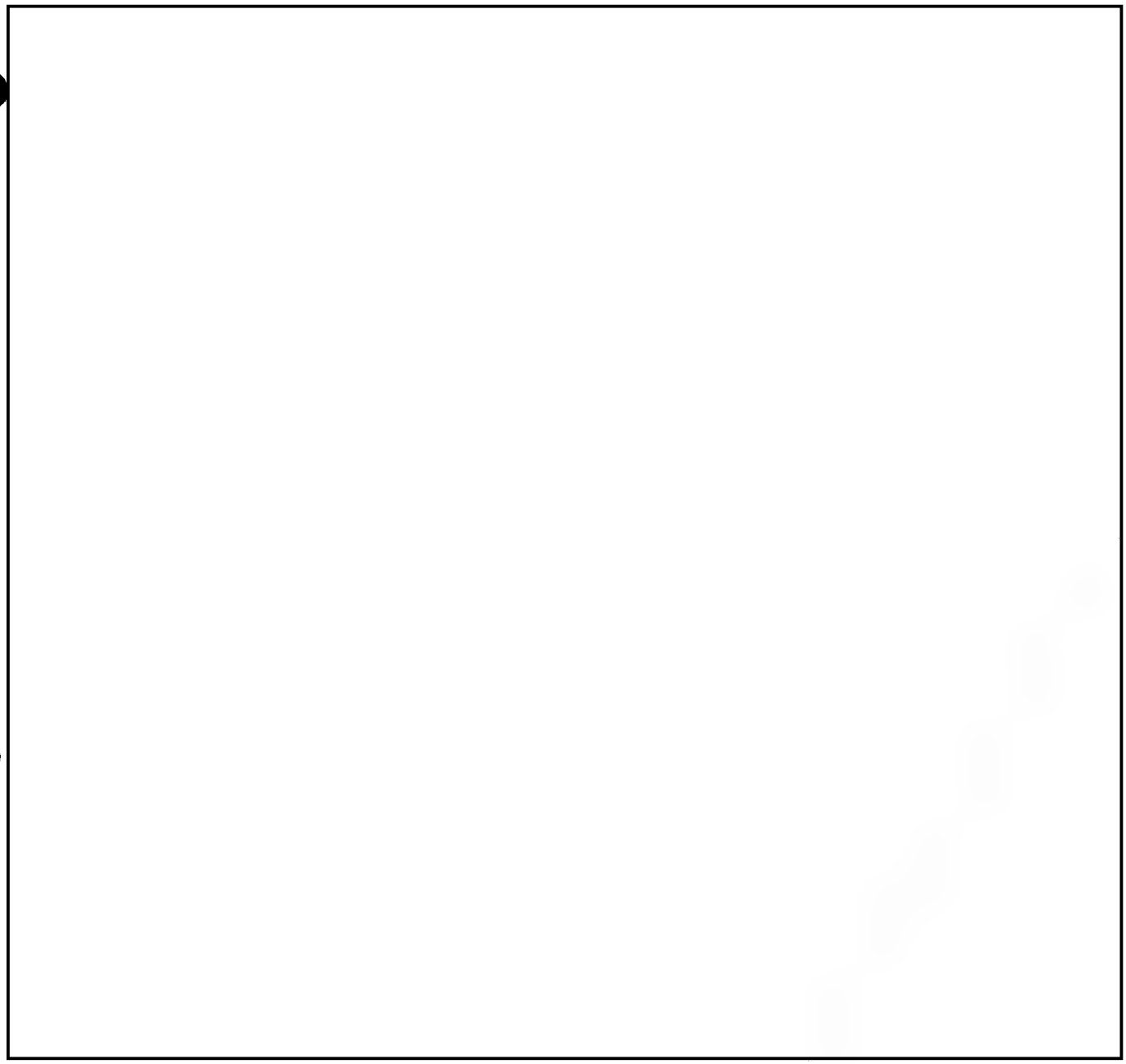
~~(C//REL TO USA, FVEY)~~ JCMA currently monitors the unclassified communications sent via the following methods:

(b)(1)
(b)(3)-P.L. 86-36

International Maritime Satellite, cellular telephone, and radio frequency. Collected communications are routed across the JCMA enterprise to analysts at Regional COMSEC Monitoring Centers at JCMA Headquarters; Menwith Hill Station, UK; Stuttgart, Germany; Camp Smith, HI; and Fort Gordon, GA. Upon receipt, communications are analyzed to determine if critical information has been disclosed or if other vulnerabilities exist.

(U~~//FOUO~~) Critical information disclosures are reported to Operational Security points of contact at the appropriate command

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



(b)(1)
(b)(3)-P.L. 86-36

National Security Agency/Central Security Service
Defending Our Nation. Securing The Future.

Defending Vital Networks

Discovering Vulnerabilities in Information Systems/Information Technology Components

(U//~~FOUO~~) Technology turnover has forced the globalization of information technology (IT) systems and has expanded the use of Commercial off the Shelf (COTS) products across the DoD and the U.S. government. This has greatly increased the challenge of discovering and mitigating vulnerabilities within U.S. IT systems. NSA/CSS strives to take a global approach to mitigating vulnerabilities by encouraging the IT industry to reduce vulnerabilities, by working with policymakers to improve policies, and by analyzing DoD networks for vulnerabilities.

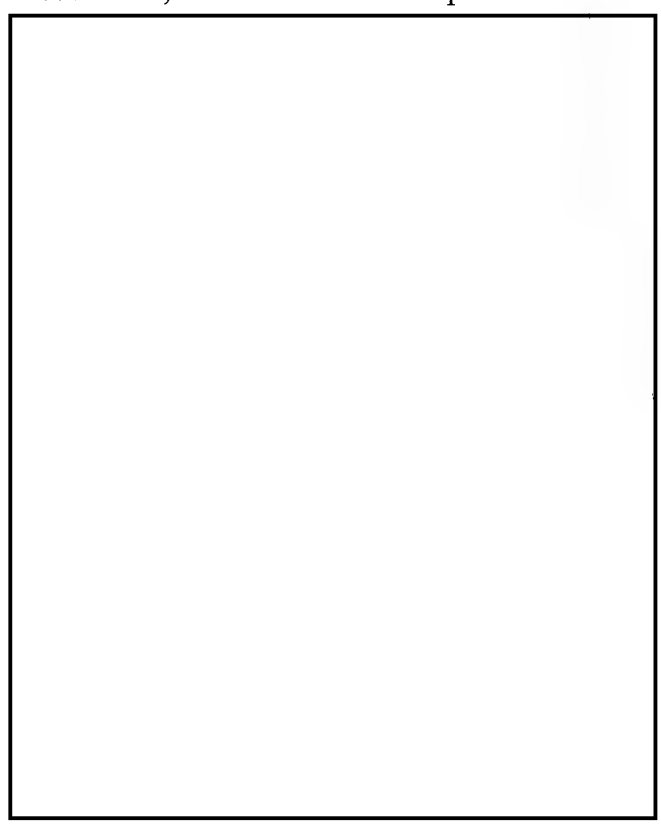
The Challenge Facing the Nation

(U//~~FOUO~~) Rapid advancement and turnover in IT systems and products have caused consumers, including the U.S. government and the DoD, to turn to COTS products to enable communications, storage, and use of data. As the demand for these goods has increased, the IT market has looked to a global model to support its products from design to production to follow-on support.

(U//~~FOUO~~) This globalization of IT goods and services has injected many foreign-made and -supported goods into the U.S. infrastructure. As the market for and supply of these COTS products has become so expansive, U.S. systems have grown in size and complexity with an infinite number of configurations, products, and security procedures. The challenge for the Nation is to determine how to find and mitigate vulnerabilities on multiple levels across these disparate systems.

How NSA/CSS Contributes

(U//~~FOUO~~) Our Vulnerability Analysis and Operations Group discovers and analyzes vulnerabilities in emerging technologies as well as the core concepts underpinning these technologies. We also conduct activities such as Communications Security Monitoring (COMSEC) and Red Teaming to find vulnerabilities in the operational environment. We translate vulnerability knowledge into summaries, trends, and root causes. We lead the community in improving security practices and we provide guidance, training, education, and standards development. (b)(3)-P.L. 86-36



(U//~~FOUO~~) NSA/CSS also seeks out vulnerability finding partners from across the government, private sector, and the international community to share information and influence security practices, guidance, training, and standards development. An example of this community leadership is the Cyber Defense Exercise which helps train the Service academies (West Point, Naval Academy, Coast Guard Academy, and Air Force Academy). The NSA/CSS Red (Computer Network Attack) and Blue (Computer Network Defense) Teams lead the community by developing standards and certifying all Service Red and Blue Teams. Additionally, NSA/CSS leads the Red/Blue (REBL) symposium which gathers all Red and Blue Teams from across the U.S. government and the DoD.

(U//~~FOUO~~) We also lead the Technical Security Countermeasures (TSCM) community which searches for physical vulnerabilities in information systems and we administer most U.S. government TSCM technical projects. Lastly, NSA/CSS works with

(b)(1)
(b)(3)-P.L. 86-36

Defending Vital Networks

Industrial Partnerships – Mitigating Vulnerabilities in U.S. Information Systems

(U//~~FOUO~~) *Keeping pace with the rapidly changing and globalized nature of Information Technology (IT) systems requires the U.S. government to use a wide variety of Commercial Off-the-Shelf (COTS) products. Use of COTS products is necessary and beneficial but it also comes with inherent risks. One way in which NSA/CSS mitigates these risks is to partner with a select group of cleared defense contractors through a program called the Defense Industrial Base (DIB).*

The Challenge Facing the Nation

(~~S//REL TO USA, FVEY~~) The U.S. Government is very dependent on its complex, dynamic, and interconnected IT infrastructure to process, store, and share vital information of all kinds. Because the federal government's systems are necessarily connected to the world's communications infrastructure, they are vulnerable to exploitation.

[redacted]

Although greater security surrounds classified networks, they too must be constantly guarded and upgraded against increasingly sophisticated threats. Vital information and systems are at risk of theft, tampering, alteration, and damage or destruction. (b)(1) (b)(3)-P.L. 86-36

The Nation's Strategy

(U//~~FOUO~~) The Nation's strategy for addressing these risks has multiple parts, covering different sectors of government-run systems and networks, and uses a variety of approaches. One essential element of this strategy is to ensure that Commercial Off-the-Shelf (COTS) products are designed and built to be as secure as possible. This can only be achieved through close cooperation between government and private industry. NSA/CSS plays a key role in this cooperative effort.

How NSA/CSS Contributes

(U//~~FOUO~~) It is essential to the security of government information that the information products and services supplied to DoD be as secure as possible. The Defense Industrial Base (DIB) program brings together a group of defense contractors to support this objective.

[redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) Working with the DIB, NSA/CSS shares threat Indications and Warning (I&W) information at the unclassified and SECRET classification levels. When they get information regarding potential threats, DIB members are able to block and recover from intrusions, fix

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

existing products, and ensure the design of future products are less vulnerable to these threats and intrusions. When we share threat I&W information, we hope to motivate DIB members to increase the security of their products prior to their implementation within DoD networks.

(U//~~FOUO~~) NSA/CSS has partnered with the DIB with a goal of fostering more secure communication and information processing technologies. We have contributed in a number of areas:

- *Standards*: We contribute to the creation and maintenance of standards managed under the auspices of numerous private-sector standard-setting bodies. We also provide input to the National Institute of Standards and Technology (NIST) and the Defense Information Systems Agency (DISA) in the development of some of their standards and guidance documents.

(b)(3)-P.L. 86-36

ADVANCING U.S. GOALS & ALLIANCES

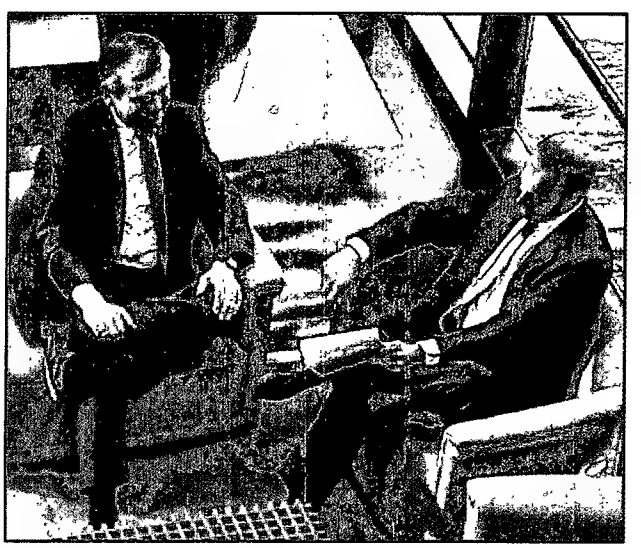
The U.S. and our allies and partners face serious national security challenges. These challenges cover a wide range that includes threats posed by powerful traditional and ascendant states, proliferation of weapons of mass destruction, the actions of extremists, and unpredictable natural disasters. Working in concert with a multitude of global partners, NSA/CSS enables the U.S. Government to meet these challenges.

Threats to our Nation

The U.S. faces serious challenges from abroad on many fronts. Leadership in responding to these challenges is the responsibility of a wide range of NSA/CSS customers, including Cabinet-level departments such as Defense, State, Energy and Treasury, as well as law enforcement agencies. NSA/CSS supports these customers, and many more, providing essential foreign intelligence that helps them carry out their missions.

Support to Negotiations and Conflict Resolution

In international relations – whether hammering out the language of resolutions in international bodies, negotiating bilateral or multilateral agreements, ranging from trade to diplomatic, or resolving difficult or dangerous situations – the better our representatives understand the relevant facts, the better they can advance U.S. goals and interests. NSA/CSS provides invaluable information supporting decision-makers and negotiators. Our customers at many levels report NSA/CSS-provided intelligence makes a decisive difference in their ability to negotiate effectively.



Countering Foreign Intelligence

Threats posed by hostile foreign intelligence elements have long been a concern, and this continues to the present day. NSA/CSS helps the Nation address these threats by penetrating the communications of adversary intelligence services. This support enables our customers to disrupt espionage and intelligence operations aimed at the U.S. and its allies.

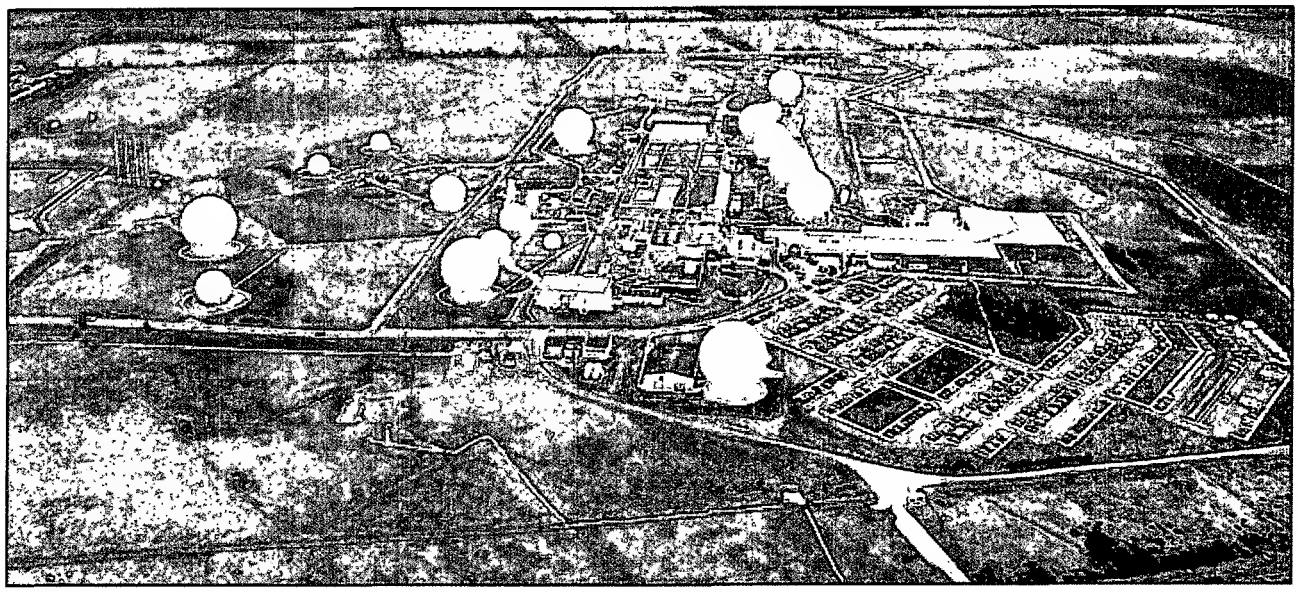
Compliance Monitoring

NSA/CSS provides intelligence critical to monitoring compliance with international agreements. Signals Intelligence can provide the first indication of a country's intent to breach an agreement, providing decision-makers warning that an area merits attention. Nuclear compliance information provided to national-level political customers, ranging from the White House to technical experts, enables them to monitor this threat and other nations' adherence to international agreements. NSA/CSS provides actionable intelligence to military customers, which assists in the interdiction of suspect shipments that violate U.N.-imposed sanctions. We also work with other Intelligence Community members to monitor time-sensitive technical data that can support or refute compliance on a range of national interests.

Countering Crime and Narcotics

Our Nation is engaged in ongoing efforts to combat international criminal activity. This includes narcotics trafficking, alien smuggling, piracy, weapons proliferation, and money laundering.

The requirements of NSA/CSS's law enforcement customers have expanded and broadened, as



terrorists use the drug trade to finance their operations and traditional criminal elements branch into activities with national security implications. We support U.S. and international law enforcement in identifying, tracking and neutralizing these rogue elements abroad.

Strengthening U.S. Ties Abroad

NSA/CSS has established foreign partnerships to advance its Signals Intelligence and Information Assurance missions. Increasingly, we work not only with traditional allies, but with new partners to exchange vital information that can secure our Nation. NSA/CSS's Information Assurance partnerships began principally as support to NATO allies and military operations, and continue today, albeit with an expanded cadre of partners. Signals Intelligence partnerships allow us to extend our reach to provide critical terrorist threat information to our military forces, embassies and interests abroad, and the Department of Homeland Security. These alliances show America in its best light: using its technical advantage to improve collective security worldwide in advancing our common interests.

Promoting U.S. Economic Interests

The Departments of State, Commerce, Treasury and Energy drive policies to support U.S. economic interests. These departments rely on the foreign intelligence information NSA/CSS provides. Foreign economic, energy, and trade issues all have significant implications for the U.S. economy.

NSA/CSS provides key information to U.S. policymakers and negotiators on the plans and intentions of foreign actors. We monitor countries that are securing or monopolizing energy in a tight market, offer insight into global positions for key trade negotiations or summits, and provide reactions to U.S. economic policies and actions to policymakers.

Supporting Military Operations

As a component of the Defense Department, NSA/CSS provides time-sensitive intelligence support to military operations. This support is provided from our sites around the world, and by personnel integrated into forward deployed forces. NSA/CSS tailors its support to each military command and has the ability to change direction as crises evolve.

Tracking Global Environmental and Health Threats

America's security interests are affected by pandemic outbreaks, environmental catastrophes, and unforeseen natural disasters. NSA/CSS responds to a variety of customers with different products and services to support U.S. efforts to address these issues. ■

National Security Agency/Central Security Service
Defending Our Nation. Securing The Future.

Advancing U.S. Goals & Alliances

SIGINT Contributions to Countering Crime & Narcotics

(U//~~FOUO~~) In today's world, the crime/narcotics/terrorism nexus is of growing importance to U.S. national security because of the obvious dangers it presents to U.S. and Coalition interests as well as implications for the Global War on Terrorism. NSA/CSS produces vital intelligence on links between criminal activity and terrorism, giving decision-makers and law enforcement the crucial insight they need to deal with the problem effectively.

The Challenge Facing the Nation

(U//~~FOUO~~) The U.S. Government is faced with the great challenge of identifying and disrupting the convergence of terrorism with criminal forces. Disparate bits of information collected or owned by one agency or another, often times, is not very useful when standing on its own. In order to be effective, the Intelligence Community has recognized, we must merge all of the intelligence produced throughout the community on a given issue. Long-standing barriers related to information sharing and ownership must be overcome in order to be successful.

The Nation's Strategy

(U//~~FOUO~~) Great strides have been made in policy and practice to improve information sharing with law enforcement and other intelligence agencies working to expose and disrupt the growing criminal/terrorism nexus. Successful prosecution of these targets requires strategic analysis that tracks the increasing danger from the nexus, while highlighting areas of vulnerability.

(U//~~FOUO~~) The ultimate goals are to

[redacted]

The Intelligence Community must continue to work together to seamlessly share information at the lowest possible classification to ensure maximum utility for law enforcement. (b)(3)-P.L. 86-36

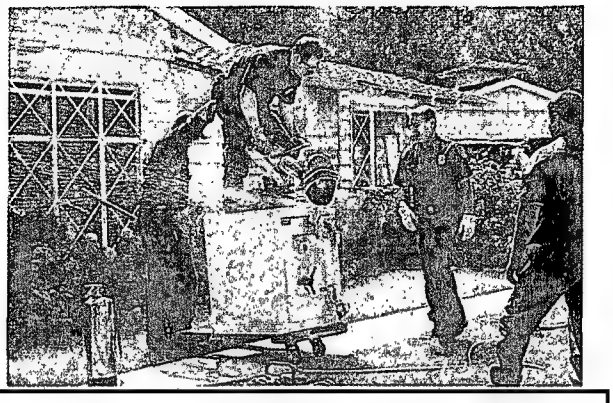
How NSA/CSS Contributes

(U//~~FOUO~~) NSA/CSS partners with a variety of customers including policy-makers at the White House, the Department of Homeland Security, State Department, and the Department of Justice; Law

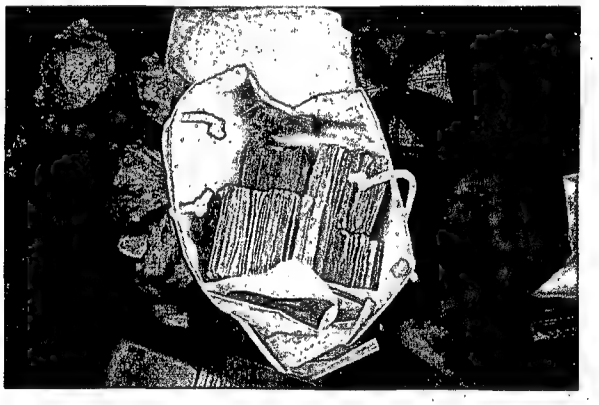
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Enforcement

and Intelligence Community



Success Stories



(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Advancing U.S. Goals & Alliances

Expanding/Broadening Signals Intelligence Foreign Partnerships

Our partners include "Second Parties" (Australia, Canada, New Zealand, and the United Kingdom) and "Third Parties" (all other nations that partner with NSA/CSS).

The Challenge Facing the Nation

~~(S//REL TO USA, FVEY)~~ It takes years to develop, build and maintain the trust needed for a first-class partnership between nations. Such partnerships represent prudent investments now that will yield benefits in the future. Ongoing information exchanges and technology sharing with foreign SIGINT partners enables NSA/CSS to

How NSA/CSS Contributes

The Nation's Strategy

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

(~~S//REL TO USA, FVEY~~) NSA/CSS continues to strengthen partnerships by providing formal and informal cryptologic analytic training aimed at improving the partners' capabilities.

(~~S//REL TO USA, FVEY~~) NSA/CSS provides SIGINT Liaison Officers (SLOs), or in-country representatives, who are vital to the success of NSA/CSS' foreign affairs program.

(~~S//REL TO USA, FVEY~~) In addition to bilateral partnerships, NSA/CSS continues to support a limited number of multilateral relationships such as SIGINT Seniors Europe (SSEUR) and SIGINT Seniors Pacific (SSPAC)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

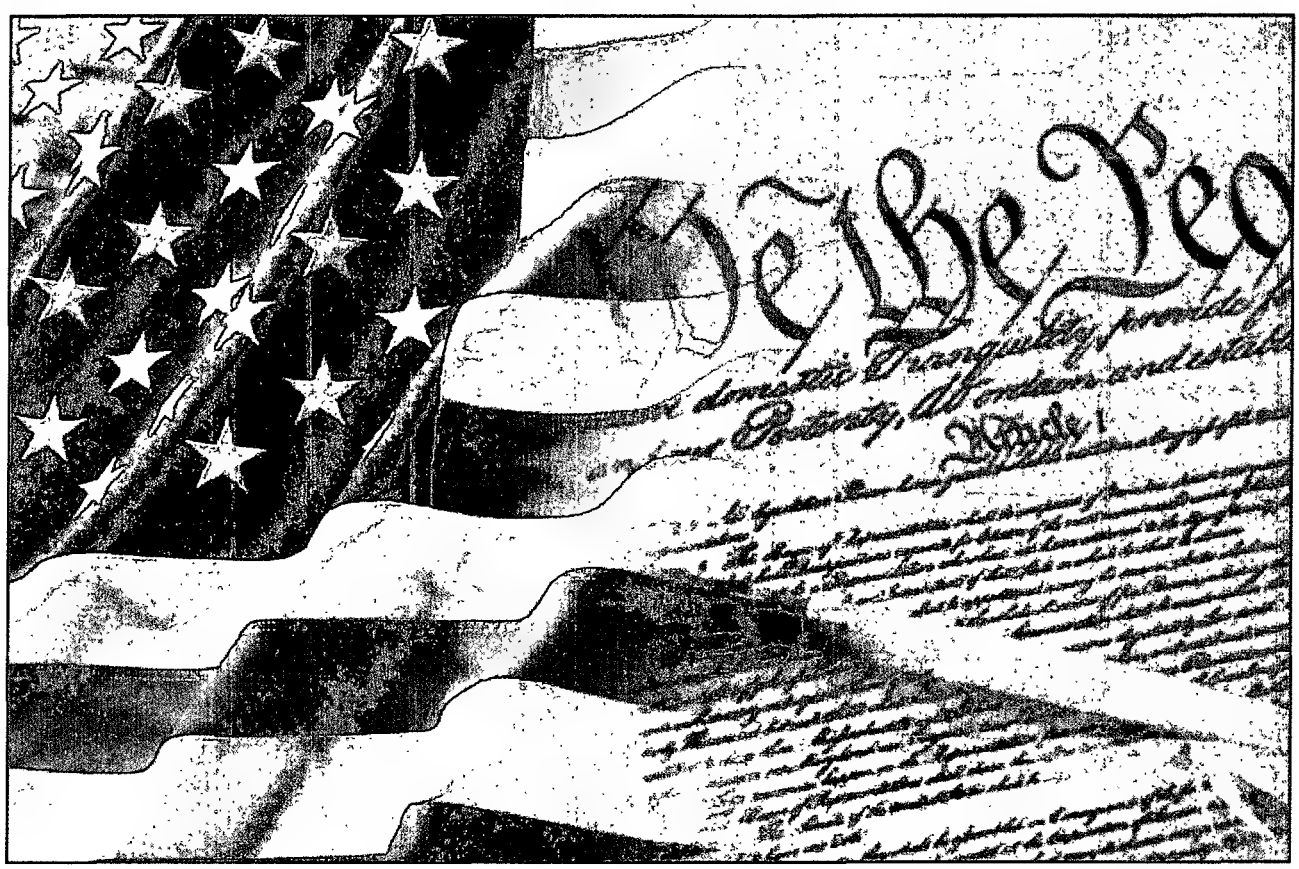
PROTECTING PRIVACY RIGHTS

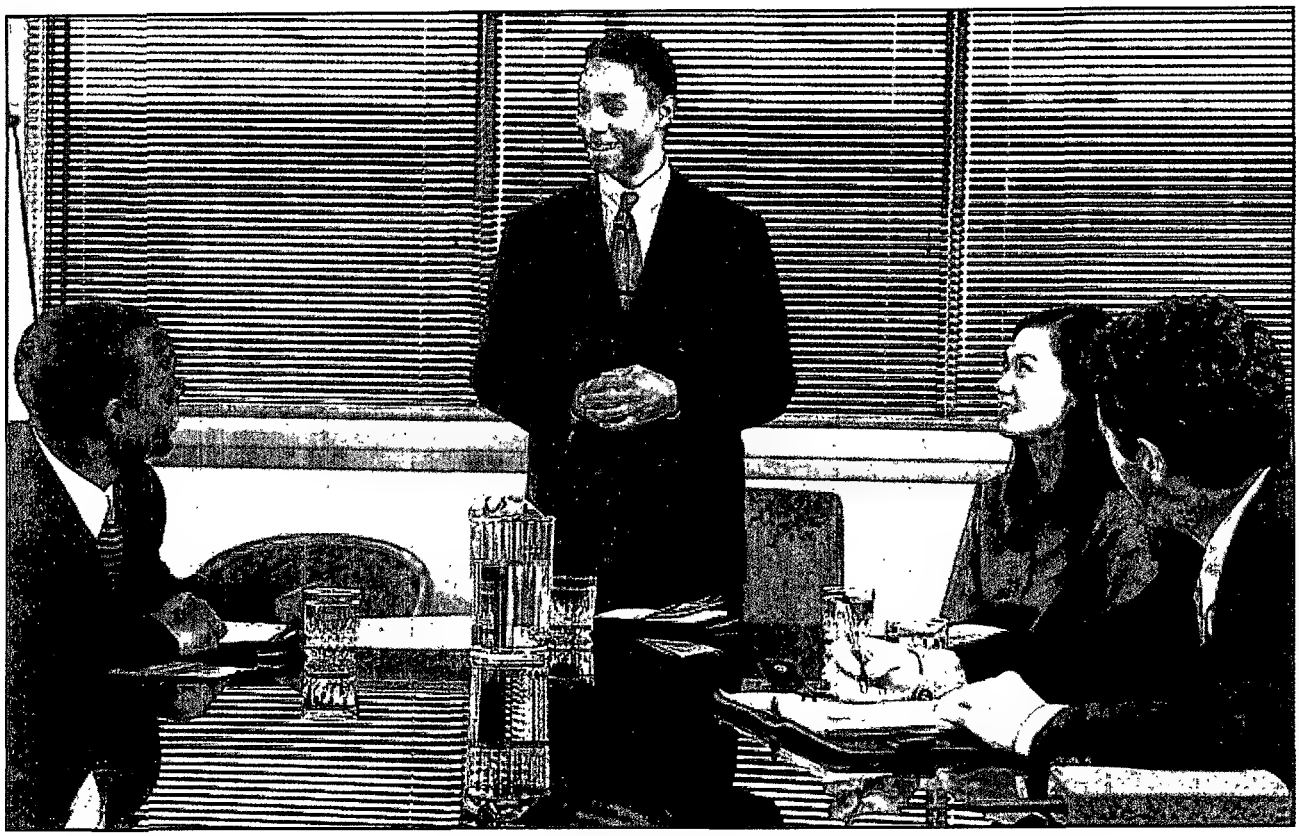
A complete understanding of NSA/CSS includes not only how the Agency helps defend the Nation, but how it protects privacy rights as an integral part of its day-to-day work, from the commitment of its people through the procedures, laws, and rules that govern its operations. NSA/CSS's missions are conducted within a legal framework that protects privacy rights. This is clearly defined, communicated to the NSA/CSS workforce, and reinforced by extensive internal and external oversight processes. As it provides and protects vital information for the Nation, NSA/CSS scrupulously observes the privacy rights guaranteed by our Constitution and laws.

Signals Intelligence

NSA conducts the Signals Intelligence mission within a framework of laws, rules, and procedures that are consistent with, and expand upon, the U.S. Constitution's Fourth Amendment requirement for the protection of individuals' privacy rights. Our personnel are trained rigorously to ensure that all these requirements and restrictions are observed. Whenever there is any indication or allegation of wrongdoing in this critical area, it is investigated, reported, and acted upon promptly and thoroughly. Our compliance processes are part of a broader oversight structure in which all three branches of the U.S. Government play key roles:

- Executive Branch: A broad range of Executive Branch entities provides oversight of the conduct of the Signals Intelligence mission. These include the President's Intelligence Oversight Board, the Department of Defense, the Office of the Director of National Intelligence, and the Department of Justice. Internally, NSA/CSS applies rigorous training, compliance, oversight, and auditing – to include active participation by its Office of





General Counsel and Office of Inspector General – to its Signals Intelligence activities.

- Legislative Branch: In Congress, the House and Senate intelligence and armed services committees authorize the funding of NSA/CSS's activities and provide congressional oversight of the Agency's work, as well as of the broader Intelligence Community. The House and Senate appropriations committees appropriate funds and also provide oversight. NSA/CSS officials regularly appear before these committees and work with their staffs to answer questions and provide insights into all aspects of our operations.

- Judicial Branch: Where required by law, NSA/CSS's work is subject to review and approval by the federal courts. The Foreign Intelligence Surveillance Act (FISA) of 1978 created a special court to help ensure that foreign intelligence collection within the U.S. is restricted to foreign intelligence targets, and that the privacy of U.S. persons is protected.. The FISA Amendments Act of 2008 modernized the FISA to embrace 21st century technologies and further protect individuals' privacy rights.

Information Assurance

NSA/CSS conducts its Information Assurance mission under a strict legal and regulatory framework. Where U.S. person information may be involved, procedures approved by the Attorney General are scrupulously followed in order to protect civil liberties and information privacy. A good example is the monitoring of official U.S. Government telecommunications for communications security purposes, which is a service we provide to military commanders and others. The Attorney General-approved procedures (and Federal law) permit monitoring with consent, and NSA/CSS ensures that personnel are notified of the possibility of monitoring and that all required consents have been obtained before such monitoring can begin. In this way, NSA/CSS respects the civil liberties and privacy of U.S. persons and fully complies with the law. ■

Protecting Privacy Rights

NSA/CSS's Signals Intelligence Mission and the Protection of Privacy Rights

(U) In accordance with Executive Order 12333, NSA/CSS is authorized to collect, process, analyze, produce, and disseminate Signals Intelligence (SIGINT) for foreign intelligence purposes to support national and departmental purposes. Because of its potential intrusiveness and the implications for the privacy of U.S. persons, such surveillance is subject to strict regulation by statute and Executive Order. The applicable legal standards for the collection, retention or dissemination of information concerning U.S. persons reflect a careful balancing between the needs of the government for such intelligence and the protection of the rights of U.S. persons, consistent with the reasonableness standard of the Fourth Amendment.

(U) In the Foreign Intelligence Surveillance Act (FISA) and Executive Order (E.O.) 12333, Congress and the Executive have codified that balancing. Both reflect deference to U.S. persons' rights by closely regulating the conduct of electronic surveillance/collection activities that either target a U.S. person or may result in the acquisition of information to, from or about U.S. persons. In order to target a U.S. person, FISA requires a court order from the Foreign Intelligence Surveillance Court (FISC). Furthermore, even if a U.S. person is not the target, NSA/CSS's SIGINT collection activities must be conducted in a manner that minimizes the acquisition, retention, and dissemination of information about unconsenting U.S. persons.

FISA Statutory Requirements

(U) FISA is the statutory regime governing electronic surveillance for foreign intelligence purposes within the United States and targeting U.S. persons regardless of location. The Act mandates the filing of an application approved by the Attorney General setting forth probable cause to believe that the target of foreign intelligence collection is either a foreign power, an agent of a foreign power, or – with respect to U.S. persons overseas – an officer or employee of a foreign power. The purpose of the surveillance must be to gather foreign intelligence information and a certification to that effect by a senior executive branch official must accompany every application.

(U) In addition, FISA requires the government to minimize the amount of information acquired or retained and prohibits, with limited exception, the dissemination of nonpublic information about non-consenting U.S. persons, consistent with the government's foreign intelligence needs. Further, specific procedures designed to effectuate the statutory minimization procedures must be adopted.*

* (U) FISA was recently amended to provide for the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Under the Act, as an alternative to obtaining an individualized court order, the Attorney General and the Director of National Intelligence may submit a certification to the FISC authorizing, subject to the approval of the FISC, targeting of non U.S. persons who are reasonably believed to be outside the United States. Minimization procedures subject to the approval of the FISC must also be adopted.

Executive Order 12333

(U) While FISA provides the statutory basis for conducting electronic surveillance for foreign intelligence purposes within the United States and targeting U.S. persons regardless of location, E.O. 12333 establishes the overall framework for the conduct of intelligence activities by U.S. intelligence agencies. E.O. 12333 prohibits the collection, retention or dissemination of information concerning U.S. persons except pursuant to procedures established by the head of the agency and approved by the Attorney General. Each of the intelligence agencies has promulgated such procedures. NSA/CSS is governed by Department of Defense Directive 5240.1-R, "DoD Activities that May Affect U.S. Persons," including a classified appendix particularized for NSA/CSS. The procedures are further enunciated within NSA/CSS through an internal directive, U.S. Signals Intelligence Directive SP0018. The procedures are designed to ensure that collection is conducted in a reasonable manner such that a minimum amount of information about U.S. persons, who are not authorized targets, will be acquired, and that no information concerning U.S. persons will be disseminated in the absence of an affirmative decision that such information is foreign intelligence information, or is necessary to understand foreign intelligence or to assess its significance.

(U) Any changes to the procedures implemented pursuant to the Executive Order require Attorney General approval, and such changes are also brought to the attention of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence as well as the Intelligence Oversight Board of the President's Intelligence Advisory Board

National Security Agency/Central Security Service

Defending Our Nation. Securing The Future.

Protecting Privacy Rights

Oversight of NSA/CSS

(U) NSA/CSS conducts its Signals Intelligence (SIGINT) and Information Assurance missions within a framework of laws, rules, and procedures that are consistent with, and expand upon, the U.S. Constitution's fourth amendment requirements for the protection of individuals' privacy rights. This legal framework assigns roles to all three branches of the U.S. Government to accomplish both external and internal oversight of NSA/CSS activities.

External Oversight

Judicial Branch

(U//~~FOUO~~) A portion of NSA/CSS's work requires the approval of the Federal courts. Specifically, the Foreign Intelligence Surveillance Act (FISA) of 1978 created a special court to regulate most foreign intelligence collection conducted within the United States, and imposed on such collection requirements designed to protect the privacy of U.S. persons. The FISA Amendments Act of 2008 modernized the FISA to embrace 21st century technologies and required some SIGINT collection formerly done under authorization from the Attorney General to be authorized by the FISC. The Court also reviews new collection certifications authorized by the FISA Amendments Act and approved by the Attorney General and Director of National Intelligence (DNI). For some sensitive counterterrorism targets, the Foreign Intelligence Surveillance Court (FISC) requires periodic reports regarding compliance with the applicable minimization procedures.

Legislative Branch

(U//~~FOUO~~) In Congress, the House and Senate intelligence committees authorize the funding of NSA/CSS's intelligence activities and provide congressional oversight of the Agency's intelligence work, as well as that of the broader Intelligence Community. NSA/CSS officials regularly appear before these committees and work with their staffs to answer questions and provide insights into all aspects of NSA/CSS operations. In addition, the FISA Amendments Act of 2008 requires that a retrospective review of the President's Terrorist Surveillance Program be conducted by the Inspectors General of agencies involved. NSA/CSS's work on that review, along with that of other agencies, must be submitted to the House and Senate Judiciary Committees as well as the intelligence committees. Finally, the House and Senate armed services committees have additional oversight and funding responsibilities with respect to NSA/CSS's Information Assurance activities.

Executive Branch

(U//~~FOUO~~) Multiple Executive Branch entities provide oversight of NSA/CSS. These include the President's Intelligence Oversight Board; the Department of Defense Office of Inspector General and Assistant to the Secretary of Defense for Intelligence Oversight; the Office of the Director of National Intelligence (ODNI) Office of Inspector General and Civil Liberties Protection Officer; and the Department of Justice. For example, under the FISA Amendments Act of 2008, the ODNI and Department of Justice conduct periodic

oversight of intelligence collection done under joint certifications of the DNI and Attorney General.

Internal Oversight

In General:

- (U//~~FOUO~~) NSA/CSS Office of Inspector General and Office of General Counsel: Internally, NSA/CSS has rigorous oversight of its SIGINT and Information Assurance activities conducted by the Offices of Inspector General (OIG) and General Counsel (OGC), and, for SIGINT, the SIGINT Directorate's Office of Oversight and Compliance. Together, these offices conduct oversight to prevent and detect violations of NSA/CSS's authorities and report on questionable activities to external oversight bodies (specifically, to the President's Intelligence Oversight Board and the Assistant to the Secretary of Defense for Intelligence Oversight). In addition, OGC provides legal advice, guidance, and assistance to all elements on compliance with NSA/CSS's authorities and restrictions. The OIG conducts a variety of reviews, audits, and investigations to promote economy, effectiveness, efficiency, and accountability within the Agency; ensure compliance with laws and regulations; and assist in detecting and preventing fraud, waste, and mismanagement in NSA/CSS programs and operations.
- (U//~~FOUO~~) NSA/CSS Managers: Managers of NSA/CSS components maintain training programs and compliance mechanisms to implement effective internal control to achieve NSA/CSS's missions and goals and provide accountability for operations.

The SIGINT Mission

(U//~~FOUO~~) The nation's SIGINT mission must be conducted in a way that properly balances the Government's requirement for critical foreign intelligence against its requirement to protect the privacy of U.S. persons. NSA/CSS has a longstanding record of strong oversight to ensure that collection, processing, retention, and dissemination activities remain compliant with the laws and regulations that govern SIGINT activities.

(U//~~FOUO~~) To ensure this proper balance is maintained, NSA/CSS has implemented a rigorous system of internal oversight procedures to ensure compliance with the laws, executive orders, regulations, and policies that mandate how NSA/CSS must conduct SIGINT activities. These procedures cover all phases of SIGINT production, from initial collection of information through the retention and dissemination of the resulting intercept. NSA/CSS oversight activities consist of five key activities:

- (U//~~FOUO~~) *Establishment of rules.* The authority and rules that govern each SIGINT activity are established before the activity begins. These include the core executive orders, laws, regulations, directives, and policies that apply to all NSA/CSS SIGINT activities. The core rules include Executive Order 12333, FISA, DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, and United States Signals Intelligence Directive (USSID) SP0018.
- (U//~~FOUO~~) *Training on the rules.* All individuals involved in SIGINT activities—including those who conduct, manage, or oversee them—are required to know the rules that govern those activities. NSA/CSS Policy 1-23 requires all SIGINT personnel to read the core SIGINT documents every year, and newly assigned personnel must read them within 30 days of assignment. Individuals who work directly with SIGINT data and those involved in activities under special legal authorities such as FISA and FAA, also must take advanced training on the

restrictions and data handling requirements associated with those authorities. This training, which must be repeated on a predetermined basis, includes instruction by NSA/CSS legal and oversight personnel, associated authorities-related readings, and a competency test that an individual must pass before the individual is permitted to participate in the activity.

- (U//FOUO) *Compliance measures.* NSA/CSS implements a combination of technical, physical, and managerial measures to ensure that SIGINT activities remain compliant with the rules that govern those activities. Technological measures make it difficult for non-compliant activities to occur. Examples of

[redacted]

(U//FOUO) Managerial controls consist of policies and procedures that are put in place to further limit the chances of non-compliant activities. Examples include identification of responsible Intelligence Oversight Officers to monitor compliance at each location where SIGINT activity takes place, the requirement for multiple levels of review prior to implementation of SIGINT collection, and mandatory review of audits to verify compliance.

- (U//FOUO) *Incident reporting.* All confirmed or suspected incidents of non-compliance with the laws, directives, or policies that govern SIGINT activities are thoroughly investigated and documented with internal overseers, including the Office of Oversight and Compliance in the Signals Intelligence Directorate, the NSA/CSS OIG, and the NSA/CSS OGC. SIGINT personnel are trained and directed to report potential incidents to these overseers immediately upon recognition in order to seek advice on, and subsequently carry out, the necessary corrective actions to remedy the problematic situation. In addition to the initial incident report, SIGINT elements submit a quarterly summary of all incidents that occurred during the quarter, along with in-depth descriptions of the causes for the incident, its impacts, and the resolution. This quarterly report also includes for tracking purposes details on

[redacted] Information from these reports is included in reports that OGC and OIG submit to external overseers, such as the Assistant to the Secretary of Defense for Intelligence Oversight.

- (U//FOUO) *Commitment to remedy non-compliant situations.* NSA/CSS ensures that the causes and impacts of individual non-compliant situations are resolved, and takes steps to identify and resolve systemic problems that may have been the underlying causes. By focusing on these causes, NSA/CSS can prevent recurrence of incidents in the future. Underlying causes can be addressed in many ways, ranging from enhanced training and

(b)(3)-P.L. 86-36

process improvements, through technical "fixes" in collection and database systems.

Culture of Compliance

(U//~~FOUO~~) NSA/CSS's successful compliance with the laws and regulations that govern its SIGINT activities is a direct result of its recognition of the importance and continued development of compliance as an integral part of the conduct of SIGINT activities. SIGINT personnel know the rules that govern their activities, know how to conduct the activity in a compliant manner, and know that each and every one of them is responsible for the compliance of the group. This environment is self-reinforcing, advocated and maintained by both managers and individuals, and results from ongoing training and guidance on proper conduct of SIGINT activities and SIGINT data handling procedures, ongoing enforcement of solid oversight practices, and managerial demonstration and positive reinforcement of compliant behaviors. It also results from a lack of tolerance for compliance lapses through implementation of active measures to remedy compliance problems, thorough documentation of procedures and practices, and establishment and maintenance of a workforce that is stable enough to ensure that new personnel benefit from the positive practices of the experienced.

NSA – A Unique National Asset

The contribution NSA/CSS makes to our national security – providing and protecting vital information – is made possible by a large and complex enterprise. It brings together a diverse, skilled, and dedicated workforce and leading-edge technology. Operating from sites in the U.S. and abroad, the men and women of NSA/CSS collaborate and share information in a network of partnerships across the U.S. Intelligence Community, the broader federal government, its counterparts in allied nations, and the private sector.

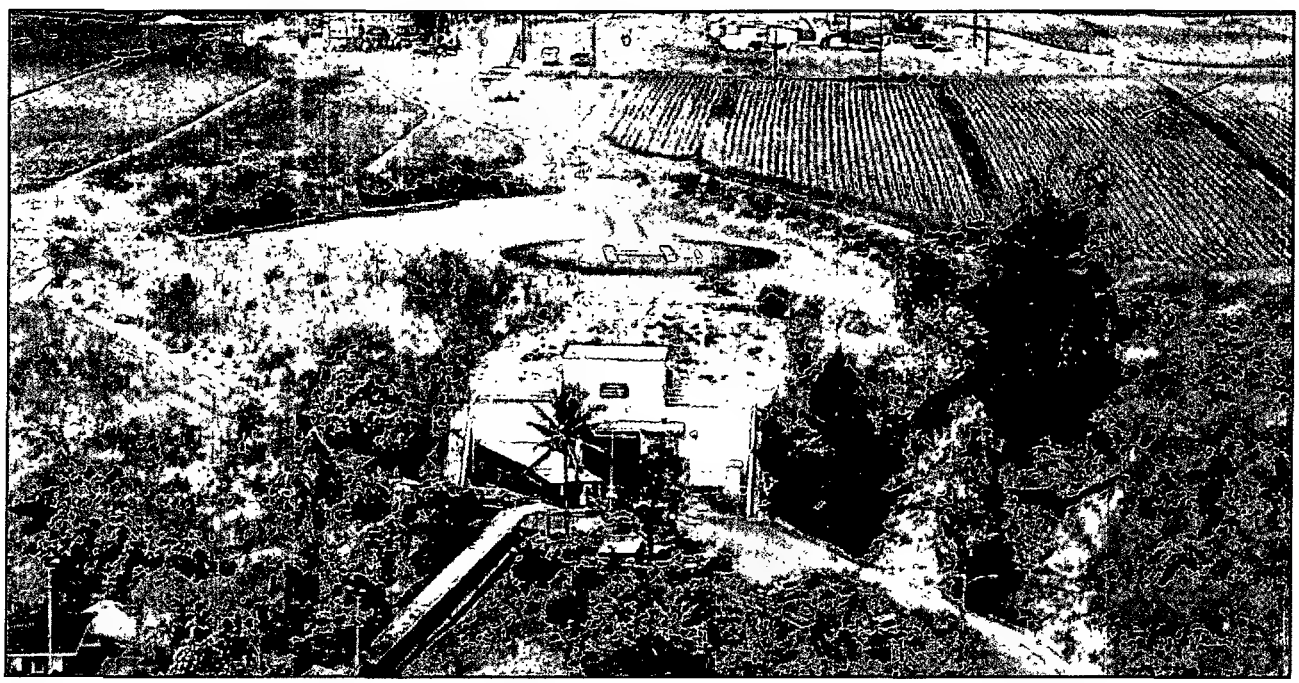
The NSA/CSS Workforce

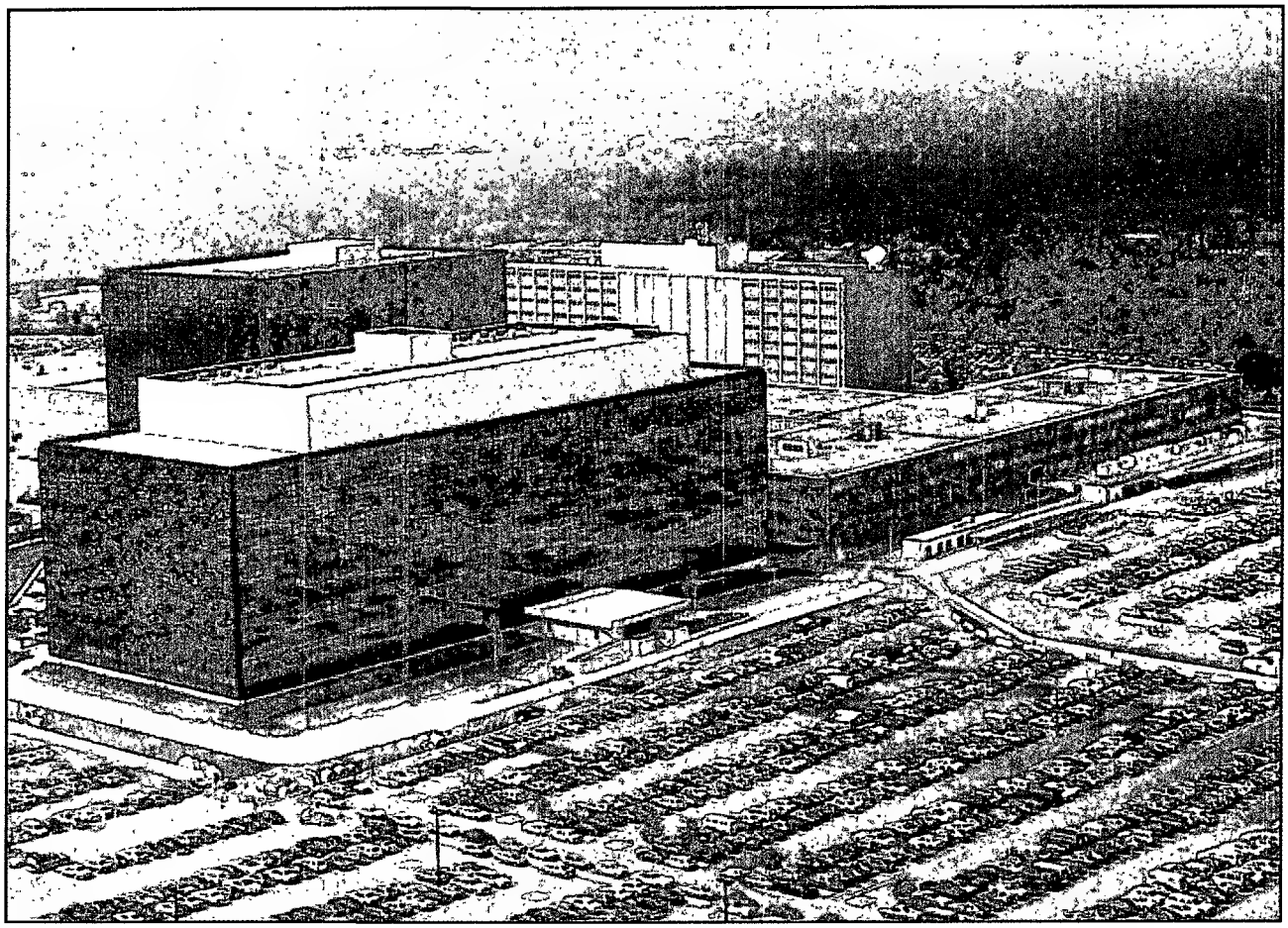
NSA/CSS employs more than 30,000 people worldwide, roughly half of them civilian and the others active-duty military. If the NSA/CSS were considered a corporation in terms of dollars spent, floor space occupied, and personnel employed, it would rank in the top 10 percent of the Fortune 500 companies.

NSA/CSS sifts through mountains of data to locate the vital information that can identify threats, shorten wars, save lives, and prevent conflicts. This is made possible by remarkable people with remarkable skills. Our workforce represents a unique combination of specialties that includes intelligence analysts, engineers, physicists, mathematicians, language analysts, computer scientists, and researchers. We recruit and hire exceptional individuals with a wide range of backgrounds and areas of expertise. We then develop and mentor them in the highly specialized skills necessary to meet the critical challenges of the NSA/CSS mission.

Leveraging Technology

Expanding global networks, increasing volumes of data, and rapidly changing technologies are challenges we face daily. In finding solutions, we frequently create new technology. NSA/CSS is a leader in the Intelligence Community in the number of patents awarded for new, innovative technological advances. Our innovative workforce has played a major role in creating new technologies in many fields, such as supercomputers and biometrics. The application of these cutting-edge technologies facilitates our ability to meet national intelligence priorities.





Our use of exclusive technology has extended NSA/CSS's reach and global presence to levels unimaginable in the past. Today, our workforce is able to share information instantly with colleagues around the world, fostering collaboration. These colleagues include NSA/CSS personnel at other sites as well as our partners.

Partnerships and Alliances

Collaboration with others is a hallmark of NSA/CSS mission accomplishment. We share information with other Intelligence Community agencies to get results that no single agency could achieve alone. Sharing intelligence we have collected with trained analysts across the community affords them the first-hand opportunity to find data they need to support their operational planning and execution in real-time.

This collaboration for the good of the Nation goes further, however. NSA/CSS provides technical and intelligence support to law enforcement, and we cooperate across international lines to protect networks and share intelligence that help keep the United States and its allies safe. We also maintain robust and productive relationships with industry and academia, accessing expertise and technology that can prove invaluable in accomplishing our mission.

Worldwide Footprint

With headquarters at Fort Meade, Maryland, our largest presence is in the Washington, D.C. area. Driven by continuity of operations concerns, NSA/CSS has chosen to place portions of its operations in other stateside locations based on proximity to key customers, access to power necessary for operating the high-technology mission, and other reasons. In addition, NSA/CSS operates collection locations, data centers, and mission activities worldwide. ■

NSA – A Unique National Asset

NSA/CSS Workforce

~~(C//REL TO USA, FVEY)~~ *Nearly 37,000 people make up the NSA/CSS workforce, with a civilian/military ratio of 52% to 48%. We recruit a diverse set of exceptional individuals from across our Nation. Working at locations across the country and the globe, they represent a truly unique combination of talent, including intelligence analysts, language analysts, mathematicians, engineers, physicists, computer scientists, researchers, and a host of supporting specialists.*

The Challenge Facing the Nation

~~(C//REL TO USA, FVEY)~~ The events of September 11, 2001 brought to the forefront many new challenges to the security of our Nation: new technologies, new languages, new global hot-spots. Our response to these and other events in the Global War on Terrorism requires highly skilled, dedicated people to collect information, detect and analyze threats, and provide the intelligence to keep our people and our infrastructure safe.

Our Strategy

(U//~~FOUO~~) NSA/CSS has aligned with the Office of the Director of National Intelligence (ODNI) to emphasize diversity as a strategic mission imperative. Central to our strategy is ensuring that a focus on diversity is an integral part of all workforce planning activities and other Human Capital initiatives.

(U//~~FOUO~~) With the commitment of our Senior Leaders, we have set our direction and will engage in continuous review of our progress on key performance measures such as increased diversity representation in core mission areas, higher pay grades, and assignments to senior positions. We will further establish NSA/CSS as a model employer for persons with disabilities by broadening our strategies to secure much needed talent through increased recruitment efforts and more creative enabling workspace solutions.

Education Level
Bachelor's Degree or higher: 68.8%
Doctorate, Professional, or Post-Doctorate Degrees: 3.9%

~~(C//REL TO USA, FVEY)~~ After September 11, 2001, NSA/CSS aggressively implemented a workforce strategy to strengthen transformation. Congress has increased our authorized strength—both NSA civilian and Service military/civilian—by 3.9% to our current authorization of 36,371 (18,849 NSA civilian and 17,522 Service military/civilian). Our strategy has not focused on growth for growth's sake, but on a measured effort to increase our capabilities.

Who we are
Women: 40.7%
Minorities: 17.7%
Persons with disabilities: 3.8%.

(U//~~FOUO~~) On the NSA civilian side of the house, we significantly increased our

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

population of language and intelligence analysts, computer scientists, engineers, and mathematicians. In addition, we have worked to staff all of our major organizations at or close to their authorized strength levels while trying to maintain balance between mission, enabler and staff functions.

Where we work

[redacted] at Fort Meade proper
[redacted] at other CONUS [redacted] at the four NSA/CSS Cryptologic Centers)
[redacted] at OCONUS locations

(U//~~FOUO~~) On the service military/civilian side, we have been no less aggressive in addressing workforce and staffing issues. We work closely with the services to notify them of our expected military manpower needs and allow them to program recruiting, accessions, training, and assignment actions appropriately. Further, we are actively working with the services on their respective human capital strategies. Where the services are de-emphasizing certain skills sets, (such as IT systems administration and logistics), we are developing strategies to transition the tasks to other portions of the overall workforce (civilian and contractors); at the same time, we seek to complement and capitalize on the skills that the services are emphasizing (such as "tactical level" analysis).

Where Agency civilians are in their careers

Average age of civilian workforce: 43.6 years
Average length of service: 16.3 years
Hired since 9/11/2001: 35.4%
Eligible to retire: 10.9%

Workforce Preparation and Development

[redacted]

(U~~//FOUO~~) NSA/CSS ensures the technical health of the workforce, both military and civilian, by aligning them with one of twenty-three Skill Communities that represent occupational groups with similar knowledge, skills, and abilities. The Skill Communities provide broad-based mentoring and career guidance through learning and development roadmaps. They also partner with our Associate Directorate for Education and Training to guide training and development opportunities that prepare our people to meet the challenges of current and future mission requirements.

Distribution of civilian workforce	
Technical and collection skill communities	
Analytic skill communities	
Organizational leadership & management	
Acquisition & business management	
Security	
Enabling activities (e.g. support services, legal, education and training, logistics, facilities, human resources, etc)	

(b)(3)-P.L. 86-36

NSA – A Unique National Asset

T3.0 Transformation: Strategic Plan for Technology

~~(S//SI//REL TO USA, FVEY)~~ *The vision of NSA/CSS Transformation 3.0 (T3.0) is to distribute our processing capabilities throughout the global enterprise and to unify our missions. To achieve these goals, we are creating a cooperative and concerted real-time exploit-attack-defend capability* [redacted] *T3.0 connects analysts, mission partners, clients, sensors, systems, and information on a global scale through a robust, secure, and distributed network.* (b)(3)-P.L. 86-36

The Challenge Facing the Nation

~~(S//SI//REL TO USA, FVEY)~~ U.S. citizens use the Internet to conduct e-commerce transactions, access public services, socialize, and learn. This same cyberspace is also the combat space for our adversaries, providing anonymity to our targets. Over 100 countries are known or suspected of conducting or developing Computer Network Exploitation (CNE) capabilities [redacted]

[redacted]

To meet the challenges and manage the complexities of today's environment, we must be able to operate on the cyber playing field and get ahead of our targets' capabilities.

How NSA/CSS Contributes

~~(TS//SI//REL TO USA, FVEY)~~ Cooperation with other government agencies and foreign partners is a key element of our strategy. [redacted]

[redacted]

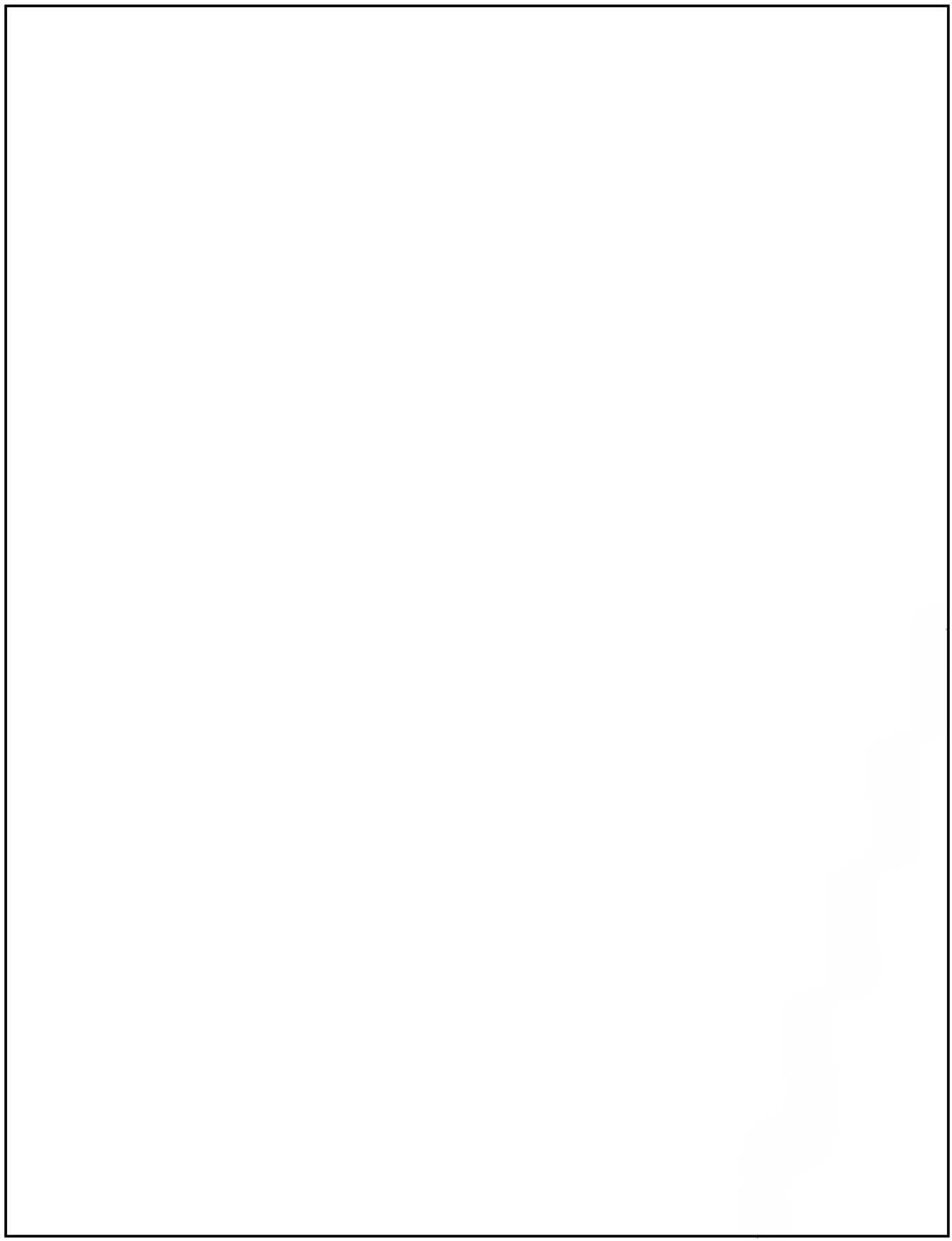
[redacted]

~~(S//SI//REL TO USA, FVEY)~~ Here at home, our Technology Directorate is designing and implementing an operational mission environment focused on enhancing mission performance and reducing information technology costs. We address these challenges on many fronts: we capitalize on existing capabilities, modernize the information technology and mission infrastructure, and integrate the exploit-attack-defend mission areas. [redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

National Security Agency/Central Security Service
Defending Our Nation. Securing The Future.

NSA – A Unique National Asset

National Security Operations Center (NSOC) Overview

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Established in 1972 in the wake of the shootdown of an American EC-121 reconnaissance aircraft over the Sea of Japan, NSOC as the NSA/CSS Mission Management Center, provides total situational awareness of the end-to-end cryptologic enterprise, national security information needs, and unfolding world events in order to optimize the worldwide cryptologic system. Agility and adaptability are keys to NSOC's success. Over the past two years NSOC has been focused on taking a much more proactive approach to anticipating world events and customer requirements while acting to ensure the NSA/CSS, enterprise-wide, is positioned to proactively respond. Some examples include executive protection, expeditionary SIGINT support, and personnel recovery.

Executive Protection

(U//~~FOUO~~) The NSA/CSS National Security Operations Center (NSOC) Executive Protection (EP) Staff is the Intelligence Community's focal point for

Expeditionary Support

~~(S//SI//REL TO USA, FVEY)~~ The

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Examples/Stories

Personnel Recovery

(U~~//FOUO)~~ When a U.S. or allied citizen is stranded in hostile territory, we initiate a Personnel Recovery (PR) effort, bringing together military, civil, and diplomatic resources to bear to return these isolated persons, (IP) to friendly control. Inter-agency officials and military commanders have a range of tools and authorities at their disposal to help them develop counter-measures to the hostage-taking threat; when the worst happens, they have access to the vital resources required to achieve a successful resolution

(U~~//FOUO)~~ NSA/CSS supports PR across the full spectrum of its definition, in

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

National Security Agency/Central Security Service
Defending Our Nation. Securing The Future.

NSA – A Unique National Asset

The Cryptologic Platform

~~*(C//SI//REL TO USA, FVEY)*~~ *Our adversaries communicate and carry out operations using complex, networked systems that span the globe.*

As telecom networks become more integrated and complex, the U.S. SIGINT system must respond accordingly,

The Network of Networks

~~(TS//SI//REL TO USA, FVEY)~~ The world communicates via an increasingly dense set of telecommunications networks supporting an expanding set of communication methods. What was once a relatively simple network of telephone and radio communications has developed into a robust set of meshed networks simultaneously mixing different media and supporting ubiquitous mobility. The computer and the telephone have merged into a single communication device providing the user with direct access to global commerce and large information repositories supported by the Internet, as well as the ability to communicate with anyone around the world.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

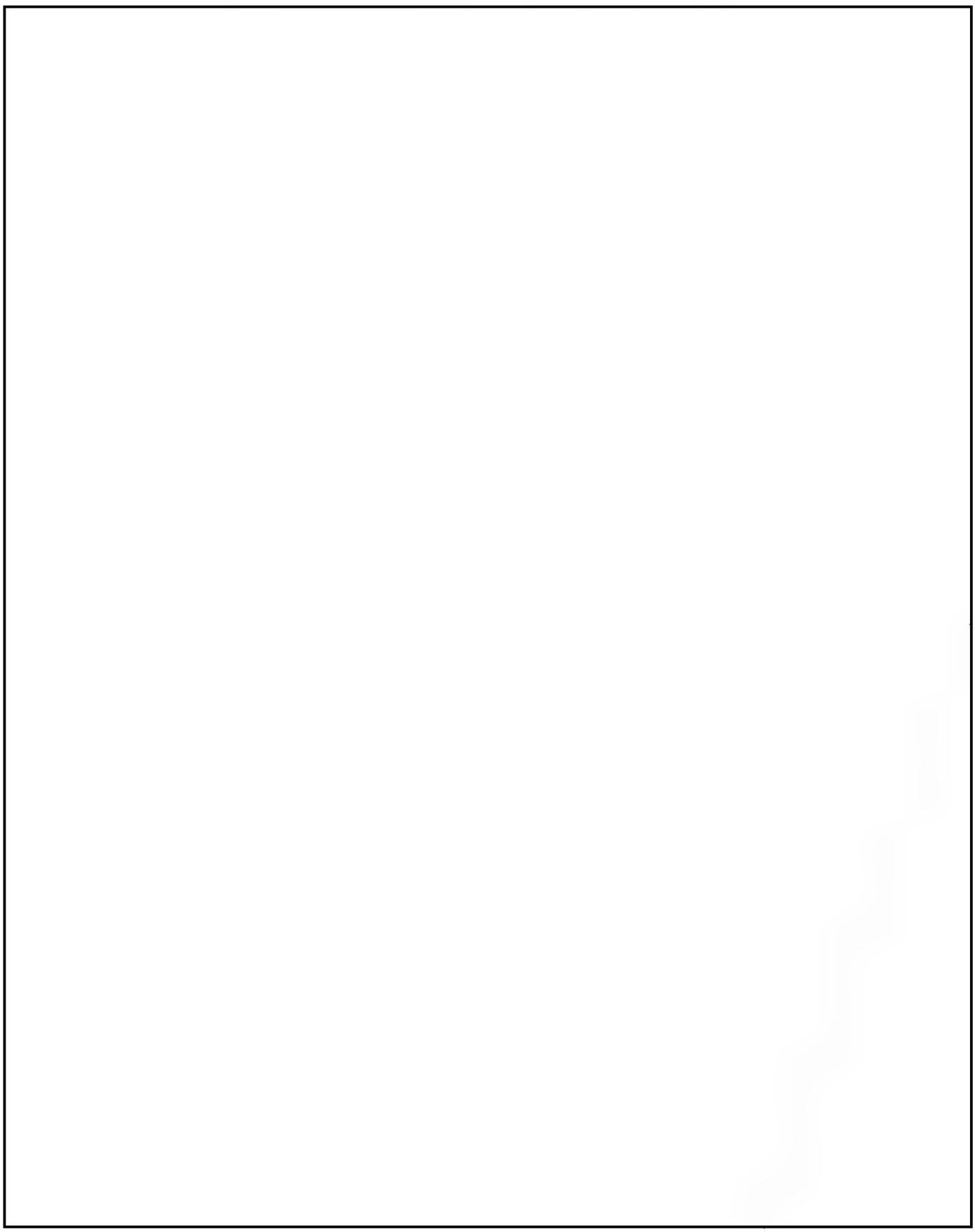
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NSA – A Unique National Asset

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NSA – A Unique National Asset

Engineering the Future: The NSA/CSS Research Directorate

(U//~~FOUO~~) Scientific advances and research breakthroughs have a significant impact on our missions. Through its Research Directorate, NSA/CSS leads and manages a research and technology development program to build new capabilities that keep pace with targets and technology. We provide technology solutions that are responsive to mission needs for Information Assurance, Signals Intelligence, and other intelligence requirements.

The Challenge Facing the Nation

(U//~~FOUO~~) Technological changes have remade our world, from the advent of the personal computer in the 1980s right through to today's reliance on cellular and satellite services. Fibers are connecting everything from neighbors to nations. Computers are in everything from credit cards to car radios. On one hand, all this makes the reach and promise of cryptology greater than ever. On the other hand, it can be very hard to find the most significant pieces of information due to a blazingly fast, astonishingly big, and inexpressibly complex set of data.

(U) The Nation is faced with a breadth and explosion of new technologies that makes it difficult to ensure that the products we use are safe from exploitation. The Nation must continue to research, develop, and deploy new technologies to keep pace with our adversaries.

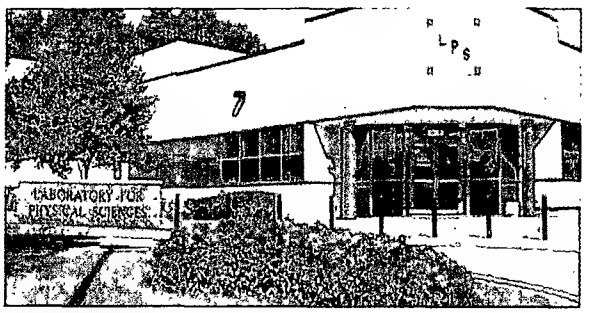
How NSA/CSS Contributes

(U//~~FOUO~~) Our customers depend on timely intelligence that gives them the competitive edge. To meet customer needs, we must continue to transform both rapidly and broadly enough to keep pace with the constantly changing target and technology environments. The NSA Research Directorate plays a key role in this transformation, maintaining close working relationships with mission customers to understand mission needs and provide solutions to current and long-term Signal Intelligence (SIGINT), Information Assurance (IA), Network Warfare (NW), and Intelligence Community customer needs.

(U//~~FOUO~~) The Research Directorate maintains an in-house research capability that truly understands the unique customer requirements of our mission areas and allows us to react quickly to satisfy urgent mission needs. For example, we are the largest employer of mathematicians in the country and are recognized as a center of mathematical excellence. We conduct research to develop solutions that are not available from any other source (commercial or government). To ensure that our program is responsive to the highest priority mission needs and avoid duplication with the commercial and academic sector, the Research Directorate has robust outreach efforts to national laboratories, industry, academic institutions, and other government research organizations within the

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Department of Defense and the Intelligence Community (IC). Employees within the NSA Research Directorate serve on national and international standards committees, conduct technical exchanges with industry, and host or participate in technical conferences/symposia across the globe.



Front Entrance of Laboratory of Physical Science Building

~~(TS//SI//REL TO USA, FVEY)~~ The Research Directorate follows a long-standing tradition in cryptology, beginning with its roots in code-making and code-breaking: we gain advantage by doing the apparently impossible. By taking advantage of the digital revolution, we have made great strides in meeting the daunting daily challenges, but there is much more to do. To keep pace with our targets and their technology, NSA/CSS must:

[redacted]

[redacted]

~~(C//REL TO USA, FVEY)~~ Since 2003, the NSA Research Program has been structured around four important mission thrusts which drive our advanced research efforts.

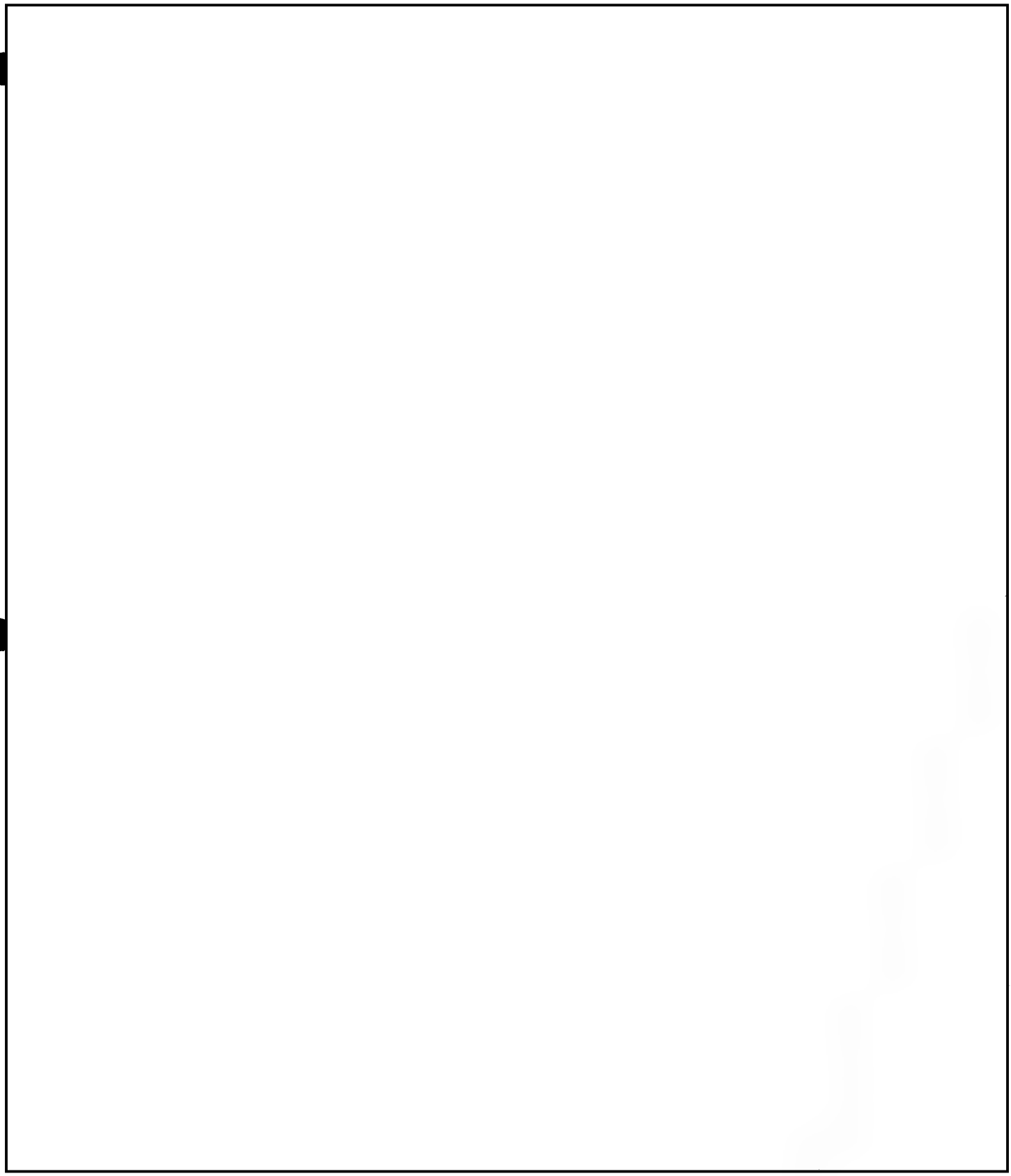
Owning the Net. This denotes our goal to dominate the global computing and communications network. Research will develop tools and techniques to access, at will, any networked device for offensive or defensive purposes.

Coping with Information Overload. We must turn the massive amount of information on the global network into a strategic asset, rather than an obstacle. Under this thrust, Research will develop capabilities to present the most valuable information, organized to make sense to analysts so that they can perform their tasks in a more efficient and effective manner.

Ubiquitous, Secure Collaboration. The focus here is to provide the techniques and technology to allow diverse users – within the government and with our industrial and international partners – to work collaboratively and securely across multiple domains and different environments.

Penetrate Hard Targets. Penetrating hard targets provides the technological solutions to enable new access, collection, and exploitation methodologies against the nation's toughest intelligence targets. The Research Directorate provides foundational and advanced mathematics that contribute innovative solutions to all of the above mission thrusts.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

National Security Agency/Central Security Service
Defending Our Nation. Securing The Future.

NSA – A Unique National Asset

U.S. Nuclear Command and Control (NC2) Support

(b)(3)-P.L. 86-36

(U//~~FOUO~~) The Director of the National Security Agency provides cryptographic products and NC2 use control code materials [redacted] *In addition, NSA/CSS provides nuclear weapon use control systems security design guidance and expertise* [redacted]

The Challenge Facing the Nation

(U//~~FOUO~~) As nuclear proliferation and the threat of terrorists obtaining, or attempting to obtain, nuclear weapons increases, the security of our nuclear weapons remains as critical as during the Cold War. The nation relies on the Department of Energy's National Nuclear Security Administration (NNSA) and the Department of Defense (DoD) to ensure that nuclear weapons remain secure and can be used only when authorized by the President.

The Nation's Strategy

(U//~~FOUO~~) The President holds authority over our nuclear stockpile. "The policy of the United States is to achieve a credible deterrent consistent with our current and future security requirements and those of our allies."[1] The NNSA and DoD have plans and procedures in place to meet this direction.

How NSA/CSS Contributes

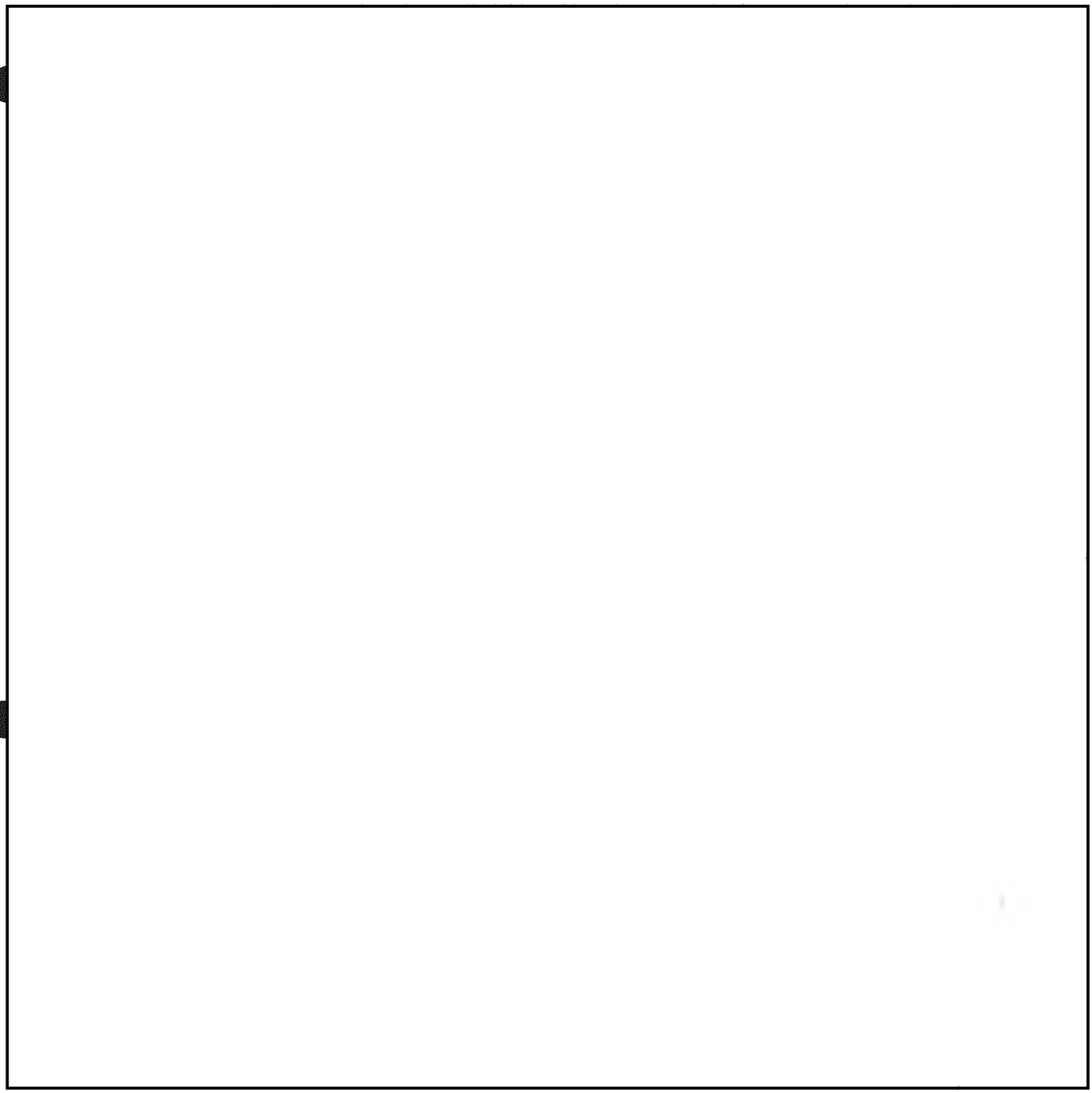
(U//~~FOUO~~) NSA/CSS provides all materials to ensure that nuclear weapons are secure in their day-to-day environments and cannot be used intentionally or accidentally without Presidential authorization. In addition, NSA/CSS produces all materials used to authorize Presidential release of these weapons to meet the national strategy.

[redacted]

(U//~~FOUO~~) NSA/CSS evaluates, in conjunction with the military departments and the NNSA, the communications security for U.S. nuclear weapon use control systems, including the cryptographic and positive control aspects of the weapon systems.

[redacted]

[1] National Security Presidential Directive–28 (NSPD-28), "United States Nuclear Weapons Command and Control, Safety, and Security," issued June 2003.



(b)(3)-P.L. 86-36

NSA/CSS Strategic Plan

June 2006

Our Vision

Global Cryptologic Dominance through National Network Advantage

We will:

- **Dominate global cryptology:** NSA/CSS will maintain its sustained competitive advantage in both technol-ogy and intellectual talent to make and break codes, and to tackle the Nation's most difficult information challenges. We will deliver and maintain a national network advantage over all who would do harm to America or her allies.
- **Secure national security systems:** Our national security systems will be secure regardless of where they are physically located.
- **Connect people, sensors, systems, and information on a global scale:** All appropriate sensors, analysts, mission partners, and clients will be connected through a robust, secure, distributed network. Emphasis will be on speed, automation, granularity, transparency, and optimization, adding cryptologic value and pushing knowledge to the edge of the entire enterprise.
- **Leverage our unique relationships with government, industry, academia, and foreign partners:** Our partnerships will enable our strategic advantage. Innovation from industry and from within, at the speed of technology, will fuel our success. We will acquire what is available, build what isn't, and rapidly decommission capabilities that are no longer operationally relevant.

Our Mission

NSA/CSS leads the community in delivering responsive, reliable, effective, and expert Signals Intelligence and Information Assurance products and services, and enables Network Warfare operations to gain a decisive information advantage for the Nation and our allies under all circumstances.

Goal 1: Mission

Deliver responsive, reliable, effective, and expert Signals Intelligence and Information Assurance, and enable Network Warfare operations, for National Security under all circumstances

- Effectively apply Signals Intelligence and Information Assurance, and enable Network Warfare operations, to defeat terrorists and their organizations at home and abroad, consistent with U.S. laws and the protection of privacy and civil liberties
- Provide cryptologic services that enable partners to prevent and counter the spread of weapons of mass destruction
- Avoid strategic surprise by achieving and maintaining capability and continuity against difficult targets
- Protect national security systems against adversary exploitation and cyber attack
- Support the global DoD mission and strengthen joint and combined military network attack operations through the provision of required intelligence and technical expertise

Goal 2: Transformation

Achieve global network dominance through the development and deployment of a new generation of globally distributed active and passive cryptologic capabilities

- Deliver, maintain, and operate network-enabled tools to strengthen analytic expertise, methods, and practices; tap expertise wherever it resides; and explore alternative analytic views
- Develop an integrated, interoperable, distributed architecture to optimize the next generation of cryptologic systems and unify exploit, defend, and attack capabilities on the common underlying infrastructure
- Develop and deploy a secure, robust information technology infrastructure to enable distributed sharing and combined operations
- Exploit path-breaking scientific and research advances that will enable us to maintain and extend intelligence advantages against emerging threats

Goal 3: People

Enhance an expert workforce to meet global cryptologic challenges

- Attract and leverage an expert and diverse workforce of mathematicians, computer scientists, engineers, signals analysts, intelligence analysts, language analysts, and staff to support the mission
- Educate, train, and develop our workforce to sustain and strengthen our critical skills
- Institute clear, uniform physical and personnel security practices and policies that allow us to work together, protect our nation's secrets, and enable aggressive counterintelligence activities
- Recapitalize physical infrastructure to promote a modern, world class work environment that safeguards the health, safety, and quality of life of our employees

Goal 4: Business Practices

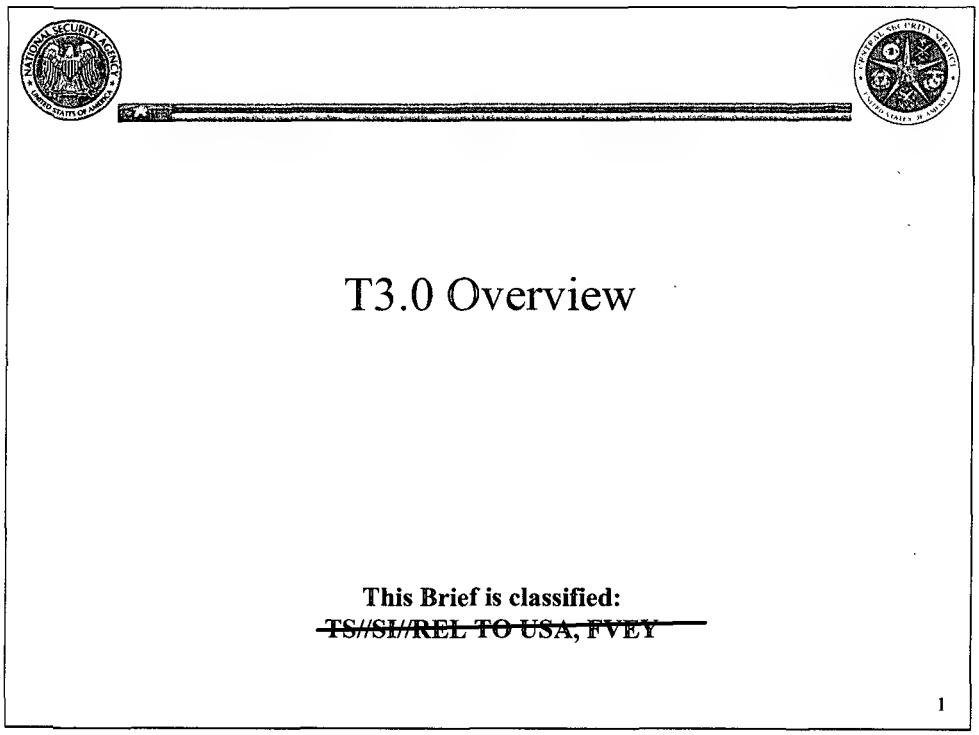
Create and integrate effective and efficient business management practices within the enterprise and with stakeholders

- Integrate budget and performance management to align investment decisions with corporate and national goals
- Develop responsive corporate business processes which rapidly allocate and realign investments and programs in an integrated way
- Strengthen foreign intelligence relationships and enhance domestic partnerships with government, industry, and academia to help us meet global cryptologic challenges

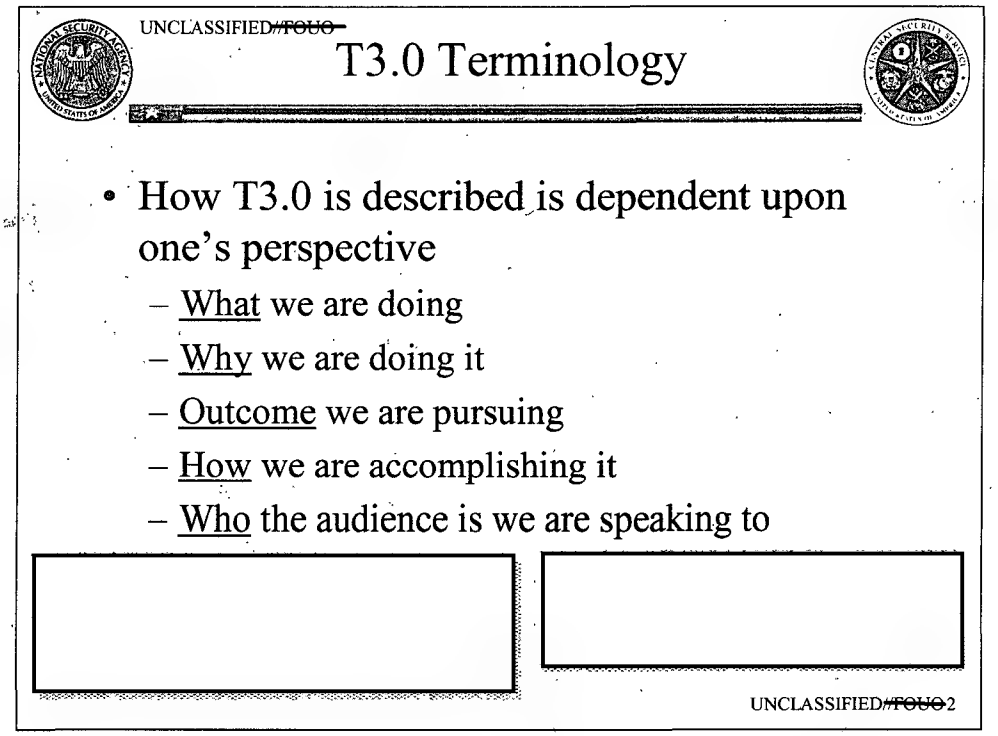
Core Values

We will protect national security interests by adhering to the highest standards of behavior.

- **Lawfulness:** We will adhere to the spirit and the letter of the Constitution and the laws and regulations of the United States.
- **Honesty:** We will be truthful with each other, and honor the public's need for openness, balanced against national security interests.
- **Integrity:** We will behave honorably and apply good judgment in all our efforts so as to avoid even the appearance of impropriety.
- **Fairness:** We will ensure equal opportunity and fairness in Agency policies, programs, and practices.
- **Accountability:** We will be accountable for our actions and take responsibility for our decisions, practicing wise stewardship of public resources and placing prudent judgment over expediency.
- **Loyalty:** We will be loyal to the Nation, the mission, and each other, weighing ideas solely on the merits and ensuring that decisions enjoy vigorous debate while being made, followed by unified implementation.
- **Collaboration:** We will cooperate with others in a respectful and open-minded manner, to our mutual success.
- **Innovation:** We will seek new ways to accomplish our mission, planning for the future based on what we've learned from the past, and thinking ahead to the best of our ability to avoid unintended consequences.
- **Learning:** We will acquire and transfer knowledge, provide the resources and training necessary for our people to remain at the forefront of technology, and individually pursue continuous learning.



Transformation 3.0 Overview


UNCLASSIFIED//FOUO
T3.0 Terminology
• How T3.0 is described is dependent upon one's perspective
– What we are doing
– Why we are doing it
– Outcome we are pursuing
– How we are accomplishing it
– Who the audience is we are speaking to
UNCLASSIFIED//FOUO 2

Externally, there has been considerable confusion as to what constitutes T3.0. In part, this confusion is the result of the fact that how T3.0 is described is dependent upon one's perspective

What (b)(3)-P.L. 86-36

Why

Outcome desired

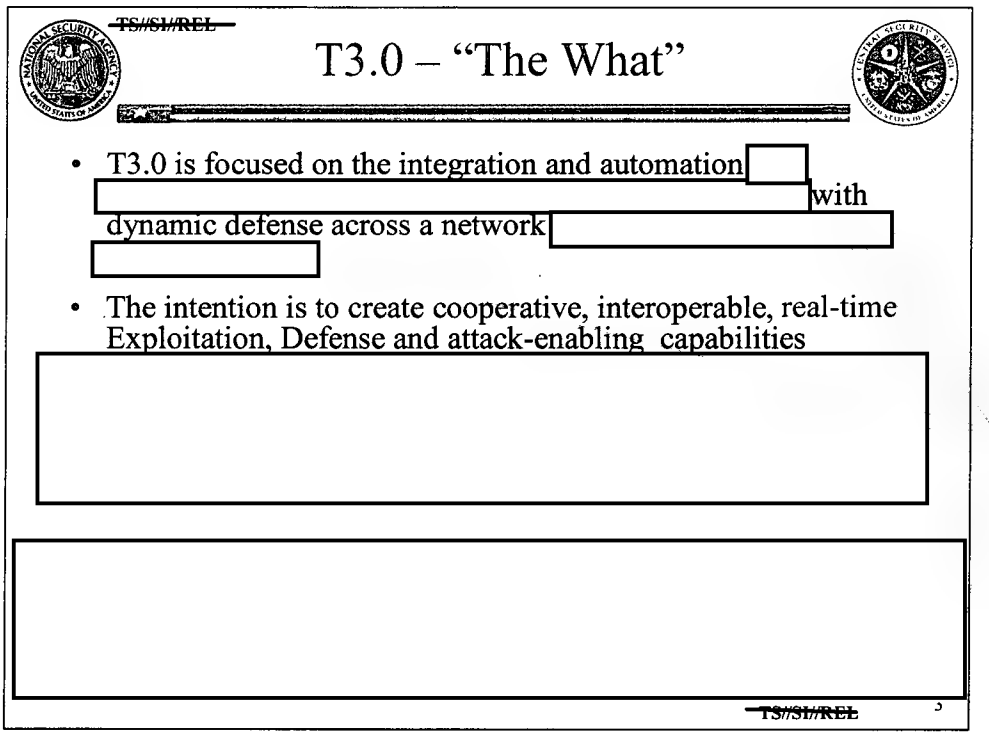
How

And just as important the **intended audience** we are speaking to …

technical, programmatic, budgetary … all want different aspects covered

An **example** of this confusion is apparent just by looking at OMB's and ODNI's request

The T3.0 Master Plan conveys a consistent framework from which all of the above discussions **(What, Why, Outcome, How)** can be derived and communicated in a consistent fashion


~~TS//SI//REL~~
T3.0 – "The What"
• T3.0 is focused on the integration and automation
with
dynamic defense across a network
• The intention is to create cooperative, interoperable, real-time
Exploitation, Defense and attack-enabling capabilities
~~TS//SI//REL~~

(b)(1)
(b)(3)-P.L. 86-36

Sufficiently explaining "**The What**" – for any cryptologic effort – usually requires a discussion of what some would consider to be technical jargon.

However, the **bottom line** is pretty clear

what is required,
what is being developed,
what will be delivered …

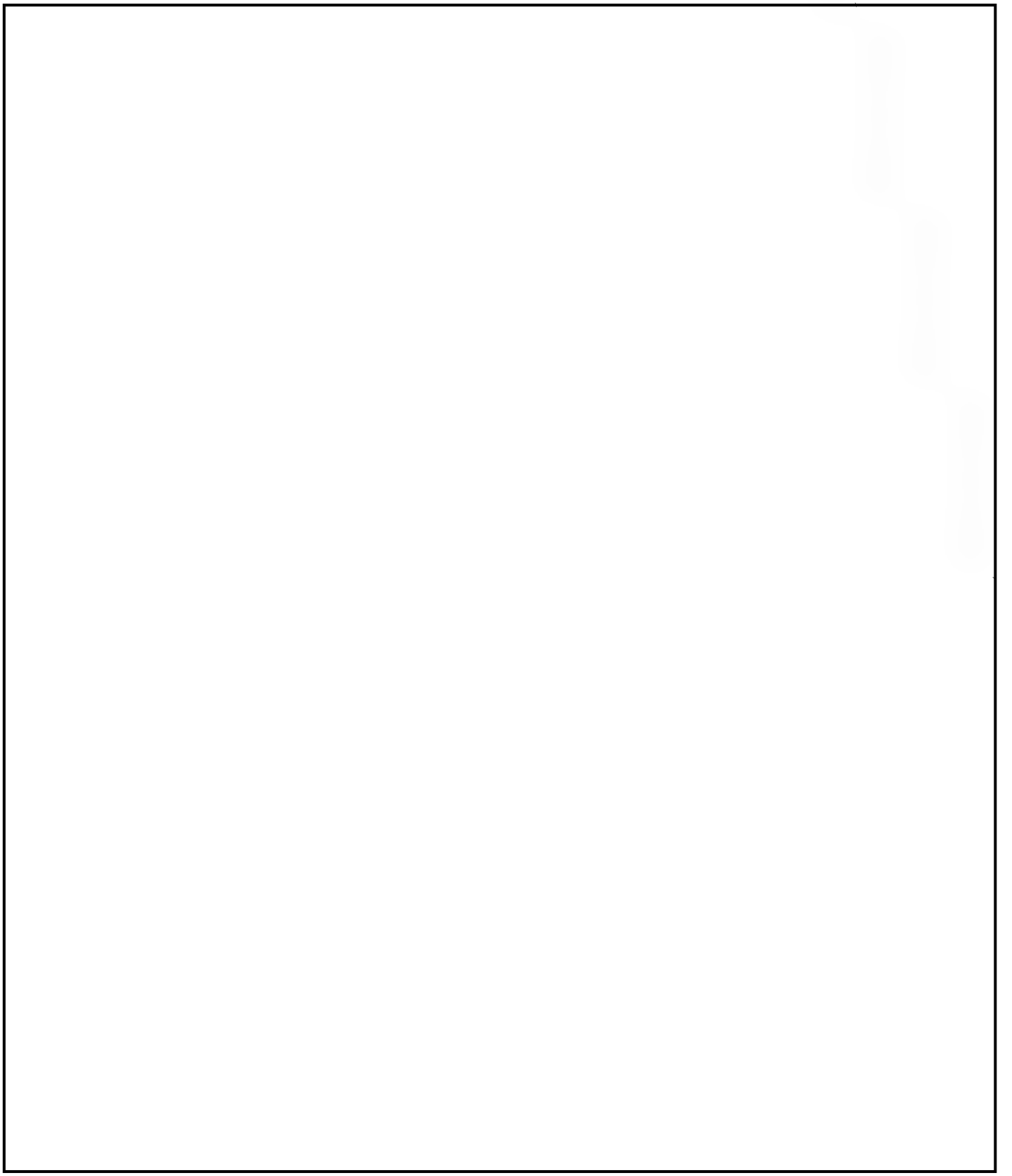
… Is an ability to ensure the nation, that the networks on which both we and our adversaries operate will serve our needs, in our best interest, not the interest of the adversary.

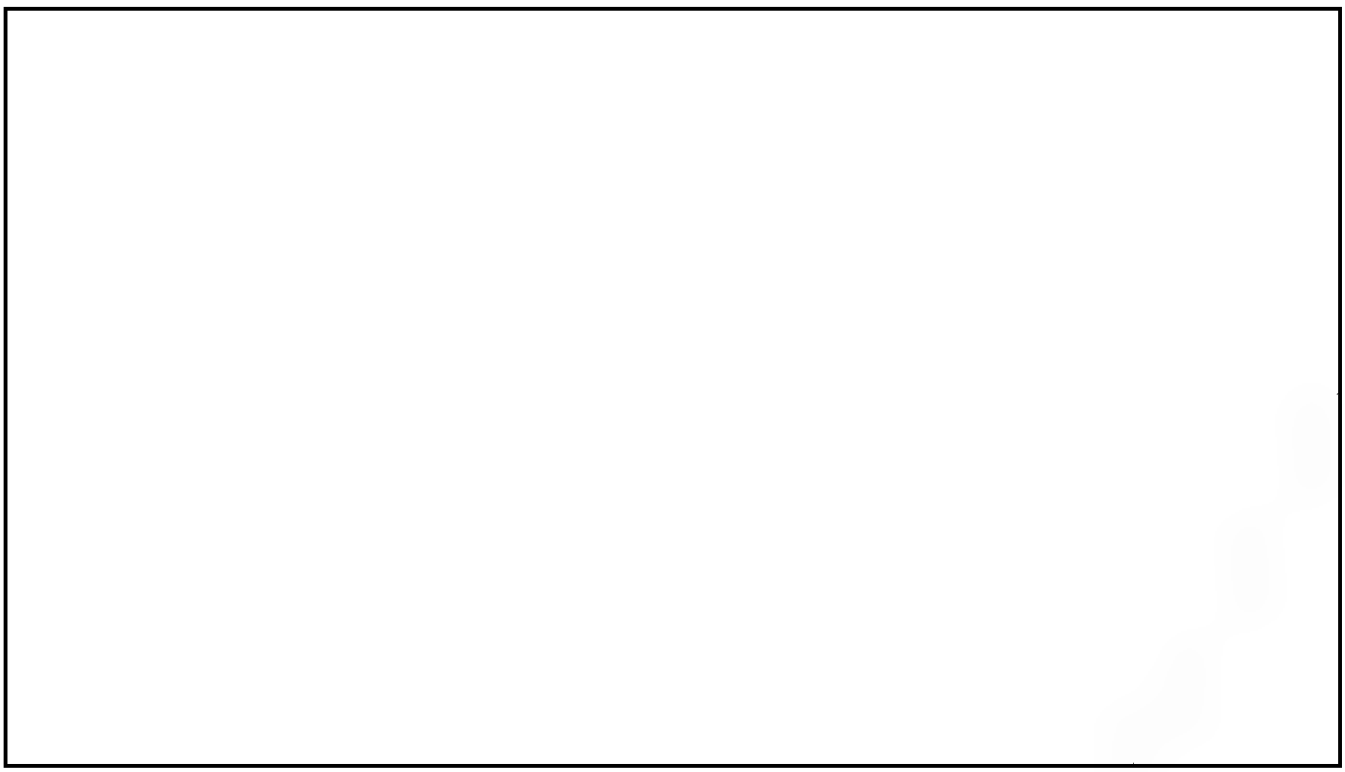
(b)(1)
(b)(3)-P.L. 86-36

• Things like:

-In effect, guarantying our national authorities the vital high round of the 21st century

(b)(1)
(b)(3)-P.L. 86-36



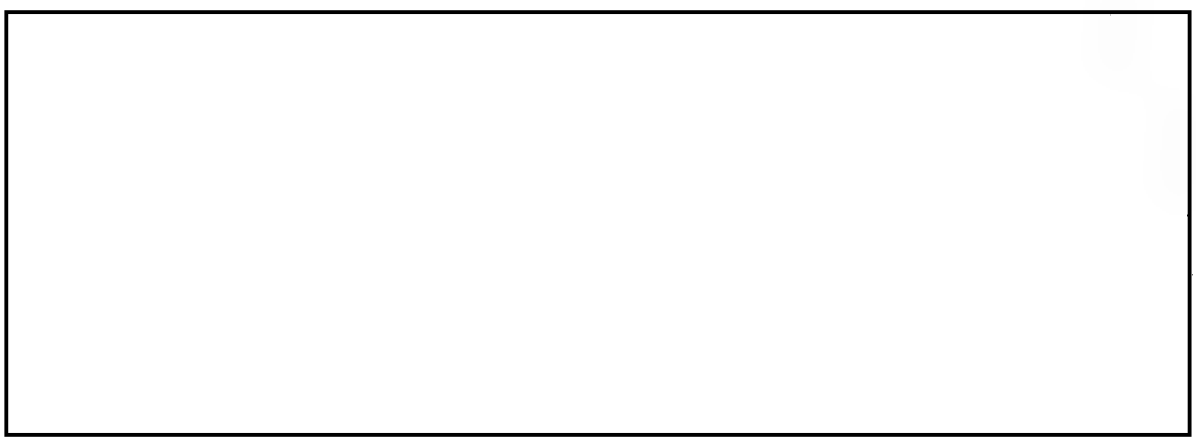


The most **compelling rationale** for advocating any new initiative – is conveying the **cryptologic benefits** that will be delivered – but that is only part of the story.

(b)(1)
(b)(3)-P.L. 86-36

The other part are the **drivers** which themselves are compelling us to transform – the **Volume, Velocity & Variety** of emerging network traffic

Cryptologic benefits are often the most visible and most compelling when discussed in the technical realm



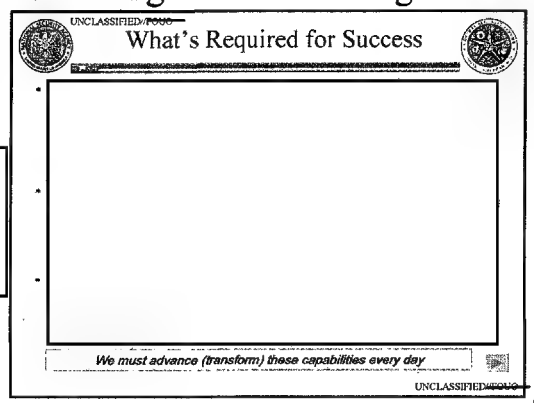
Are all **compelling rationales** that can be appreciated and understood, ….. even by an external audience that is not technically proficient

(b)(1)
(b)(3)-P.L. 86-36

UNCLASSIFIED~~//FOUO~~

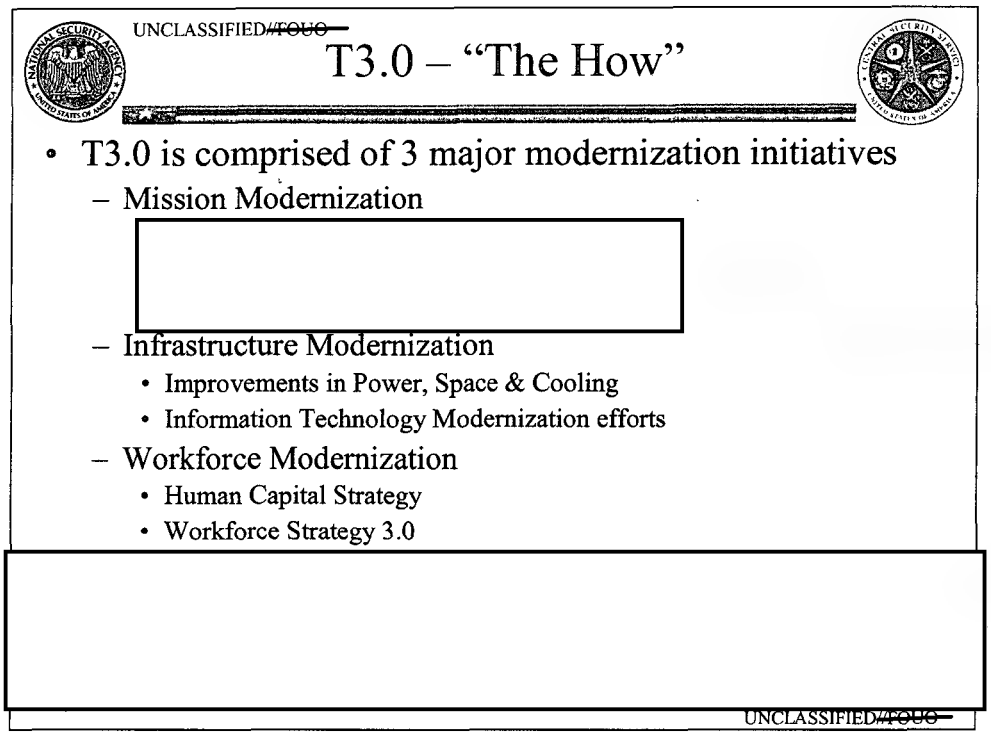
T3.0 – "The Outcome"

- T3.0 is a comprehensive constellation of NSA mission and support activities that together will establish a collaborative real-time system of people, processes, and technologies for achieving NSA/CSS' vision of global cryptologic dominance



6

UNCLASSIFIED~~//FOUO~~


UNCLASSIFIED//~~FOUO~~
T3.0 – "The How"
• T3.0 is comprised of 3 major modernization initiatives
– Mission Modernization
– Infrastructure Modernization
• Improvements in Power, Space & Cooling
• Information Technology Modernization efforts
– Workforce Modernization
• Human Capital Strategy
• Workforce Strategy 3.0
UNCLASSIFIED//~~FOUO~~

(b)(3)-P.L. 86-36

From an external perspective, "The **How**" is the meat of the story.

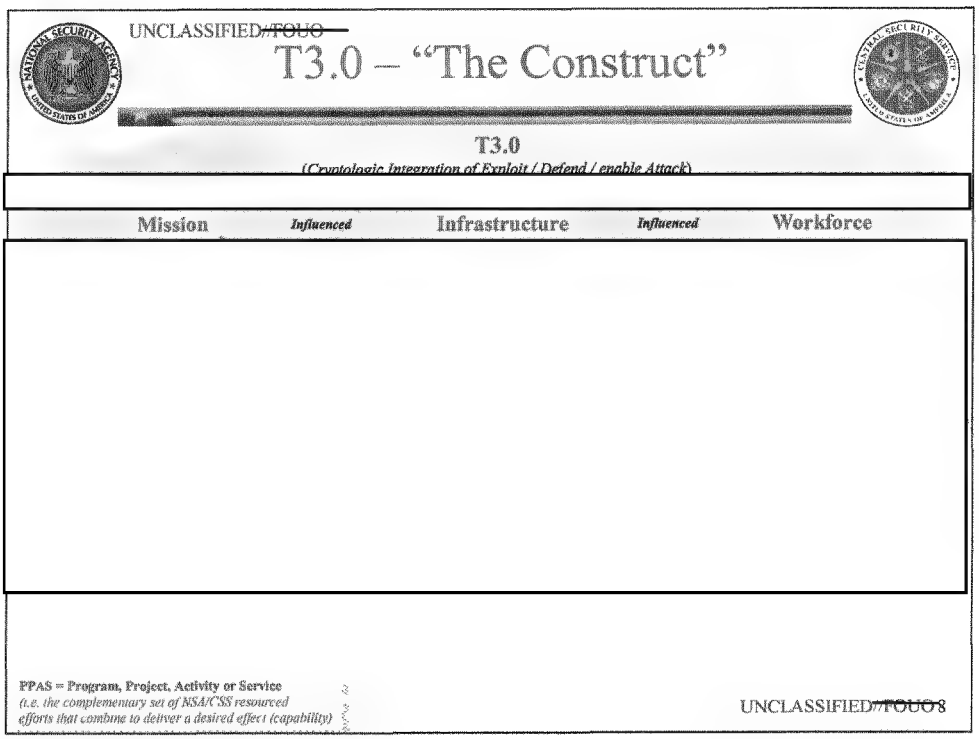
It is this aspect of T3.0 that generates the most questions from our external audience – and it is this area of discussion that – **according to our external overseers** – we fail to articulate a clear, consistent story as to what constitutes T3.0

They continually ask us **C/S/P Concepts** such as:

- How are we assuring sufficient fiscal discipline,
- Ensuring time constrained delivery … of
- Effective & Suitable capabilities, linked to national & corporate strategy

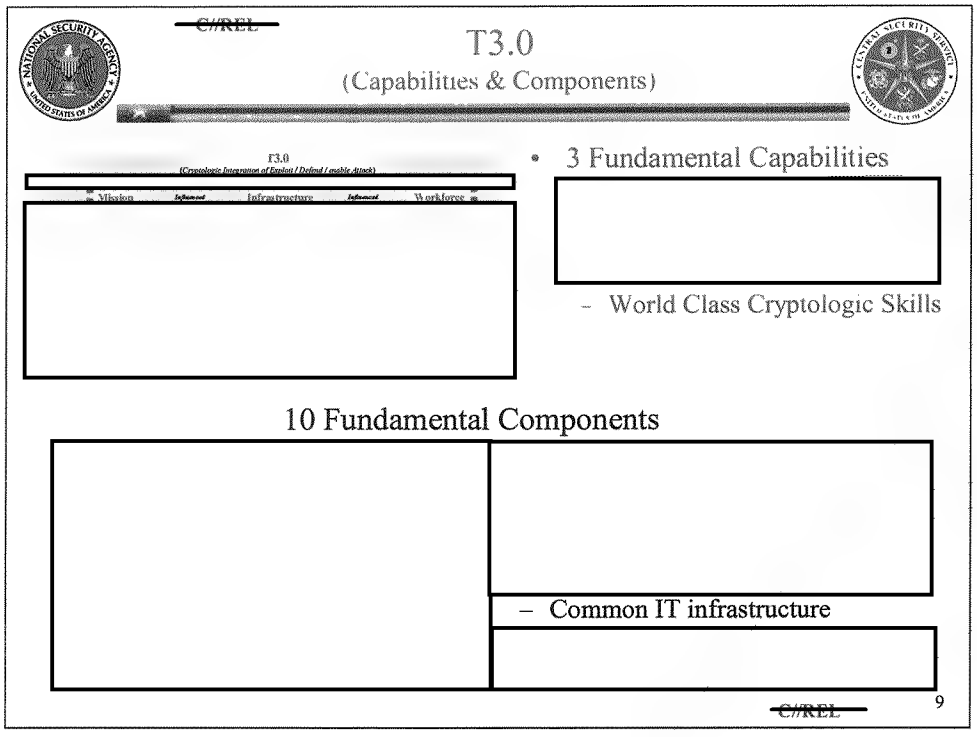
-as demonstrated by sufficient **measures of performance**

The remainder of this briefing – and indeed the majority of the T3.0 Master Plan – is focused on this very subject



(b)(3)-P.L. 86-36

T3.0 is an initiative that allows for the cryptologic integration of various Exploit/Defend and enable Attack (E/D/eA) capabilities across the UCS



(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L.

Consistent with the recently matured "Cascading T3.0" briefing series located on the Directorate Services & Communications web site ....

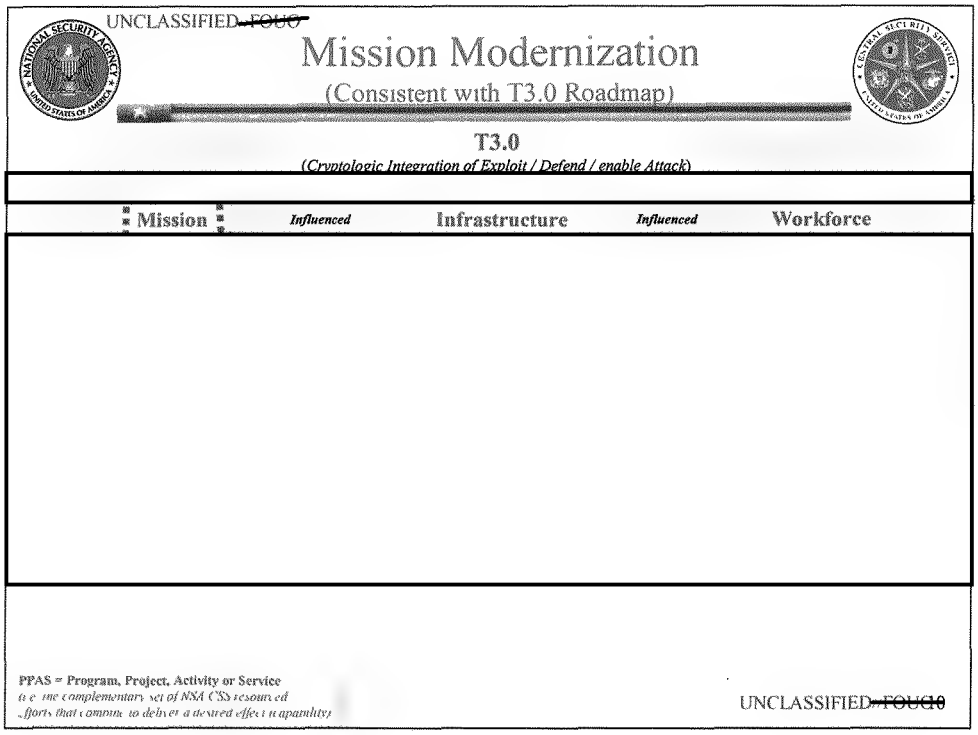
The T3.0 Master Plan conveys **three fundamental capabilities** that must be realized by the T3.0 initiative:

and

•World Class Cryptologic Skills

It also conveys that these capabilities are dependent upon **10 fundamental Components,** many of these you may be familiar with:

•Common IT infrastructure



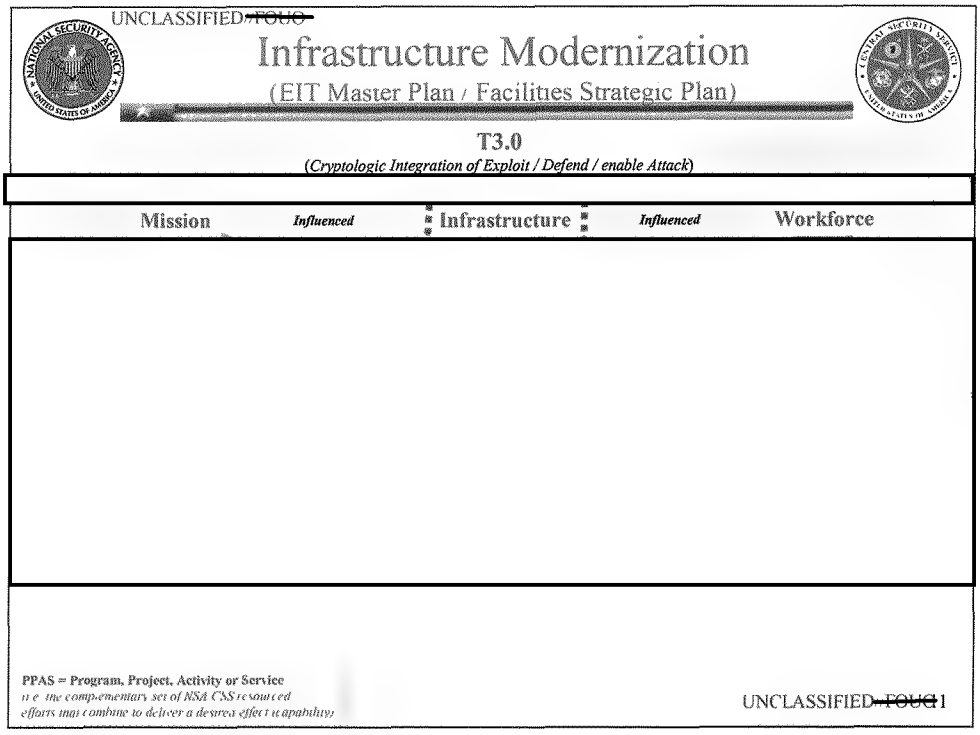
(b)(3)-P.L. 86-36

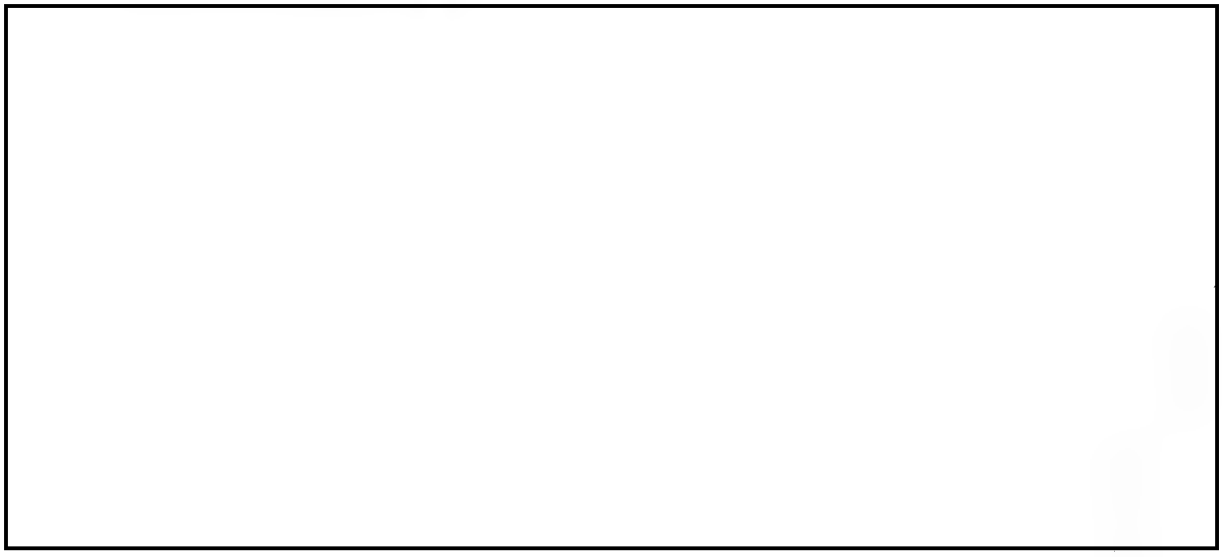
Mission Modernization involves

The key components of the Mission Modernization initiative include:

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36





•Power, Space & Cooling (PS&C) is one part of a broader NSA effort to address deficiencies in NSA's mission and support infrastructure,

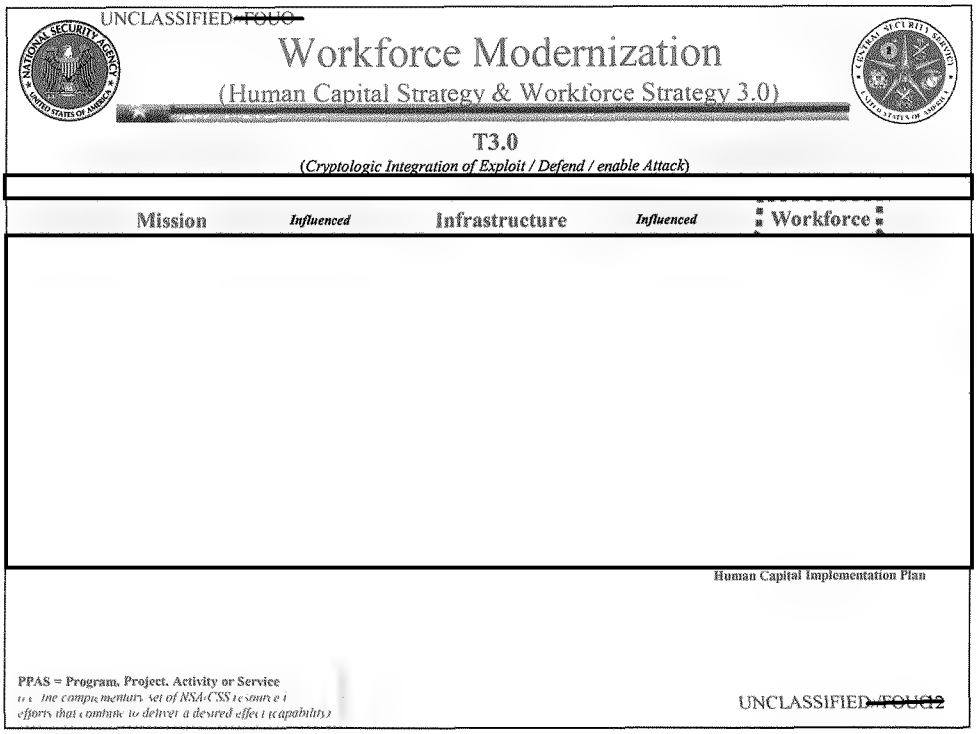
- As conveyed by the PS&C Management Roadmap and the Facilities Strategic Plan (FSP);

•The other part is Information Technology Modernization,

- As conveyed by the IT Services Initiatives Roadmap and the Enterprise IT Master Plan (EIT)

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36



As NSA transforms, changes in the way we operate, collaborate and meet emerging mission requirements demand that we better understand the influence of transformation on the total NSA/CSS workforce

The key components of Workforce modernization include:

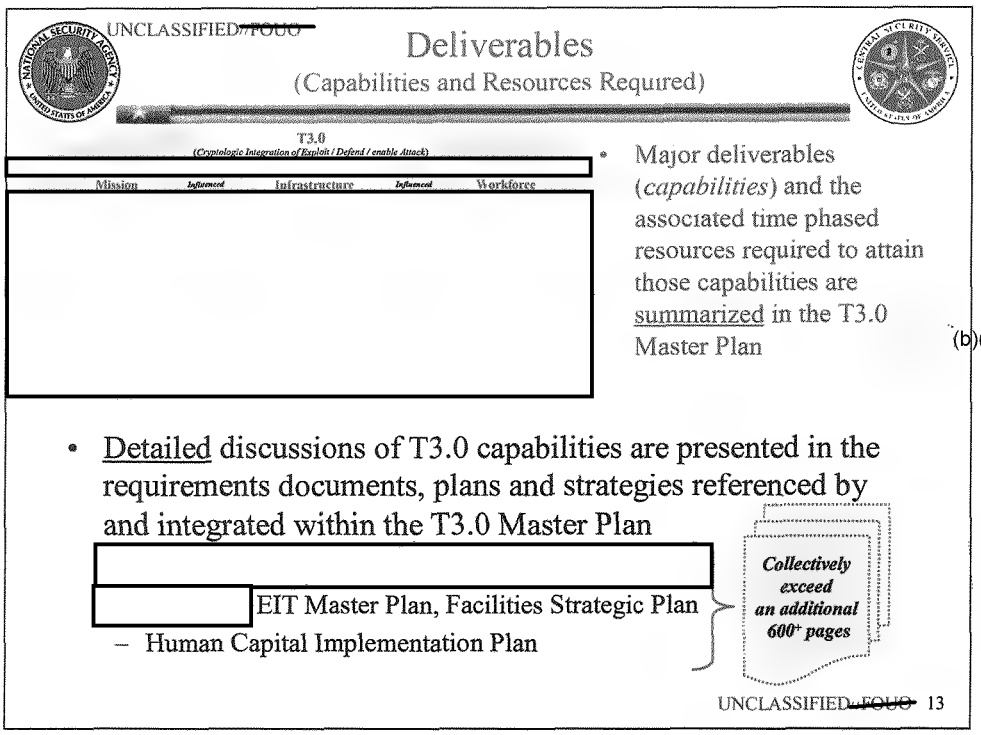
•Human Capital Strategy (**HCS**):

- A **blueprint for creating a skilled workforce** that meets the Agency's goals & objectives as it aligns people, leadership and performance with the NSA/CSS mission

•**Workforce Strategy 3.0**:

-Describes the future mission essential skill sets the NSA workforce must fill in terms of eight broad areas or "**Key Transformation 3.0 Workforce Imperatives**"

•These strategies are now in the process of being made **actionable** by the Human Capital Implementation Plan (**HCIP**) recently drafted:


UNCLASSIFIED//FOUO
Deliverables
(Capabilities and Resources Required)
T3.0
(Cryptologic Integration of Exploit / Defend / enable Attack)
Mission
Influenced
Infrastructure
Influenced
Workforce
• Major deliverables (capabilities) and the associated time phased resources required to attain those capabilities are summarized in the T3.0 Master Plan
(b)(3)-P.L. 86-36
• Detailed discussions of T3.0 capabilities are presented in the requirements documents, plans and strategies referenced by and integrated within the T3.0 Master Plan
EIT Master Plan, Facilities Strategic Plan
– Human Capital Implementation Plan
Collectively exceed an additional 600+ pages
UNCLASSIFIED//FOUO 13

Both OMB and ODNI requested to see ....

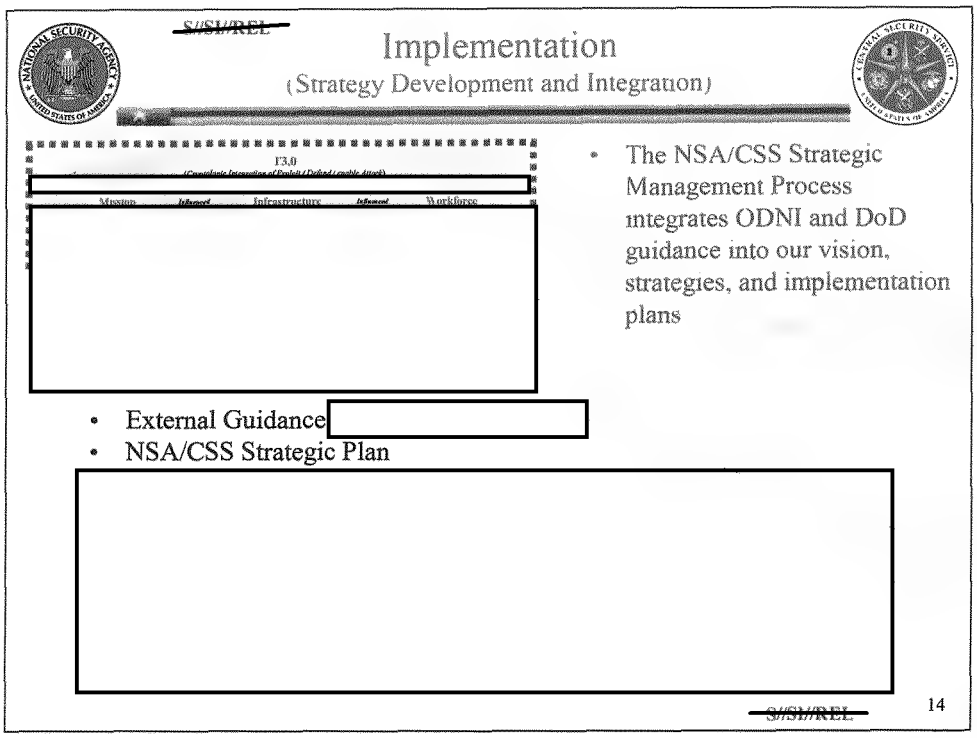
Major deliverables (**capabilities**) and the associated time phased resources required to attain those capabilities are **summarized** in the T3.0 Master Plan

•IT and PS&C summarized and derived from their stand alone plans

•Workforce, consistent with the emerging HCIP

- *Currently lacks resource allocation*

The T3.0 Master Plan notes that **detailed discussions** of T3.0 capabilities are presented **within** in the **various requirements documents**, plans and strategies referenced by and integrated within the T3.0 Master Plan



(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

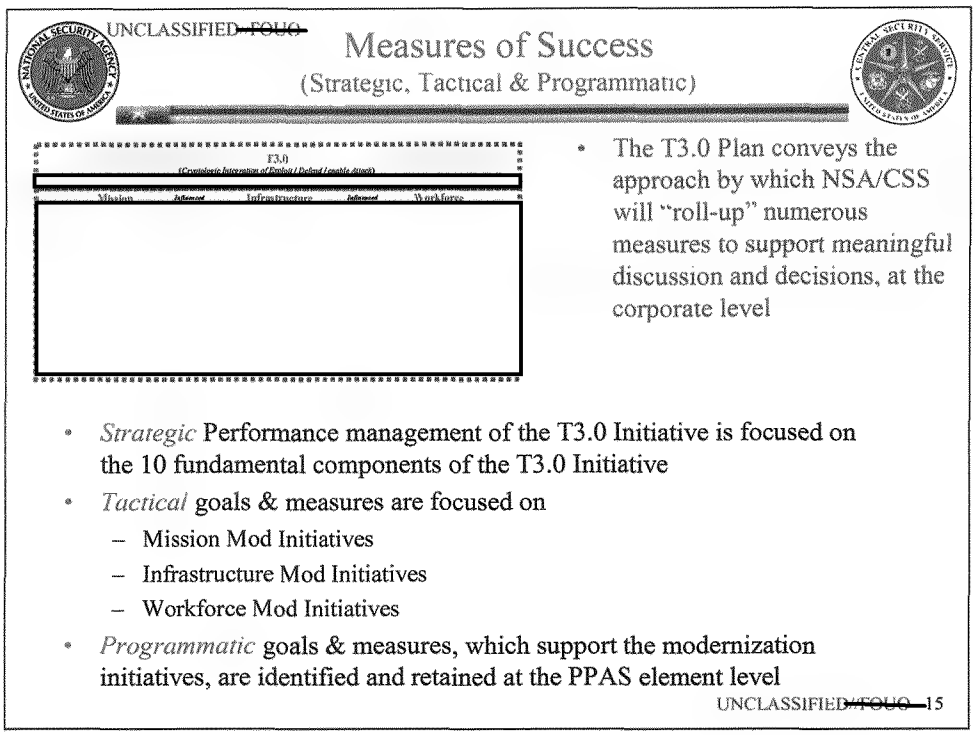
In building the FY09 Program … The NSA/CSS Strategic Management Process integrated ODNI and DoD guidance into our vision, strategies, and implementation plans

This guidance influenced our investment decisions across the enterprise to mitigate current and emerging political and technological threats

The planning, programming and integration of T3.0 initiatives presented in the FY09-13 program spanned several months

•External Guidance

•NSA/CSS Strategic Plan


UNCLASSIFIED//FOUO
Measures of Success
(Strategic, Tactical & Programmatic)
T3.0
Mission
Influenced
Infrastructure
Influenced
Workforce
• The T3.0 Plan conveys the approach by which NSA/CSS will "roll-up" numerous measures to support meaningful discussion and decisions, at the corporate level
• Strategic Performance management of the T3.0 Initiative is focused on the 10 fundamental components of the T3.0 Initiative
• Tactical goals & measures are focused on
– Mission Mod Initiatives
– Infrastructure Mod Initiatives
– Workforce Mod Initiatives
• Programmatic goals & measures, which support the modernization initiatives, are identified and retained at the PPAS element level
UNCLASSIFIED//FOUO 15

(b)(3)-P.L.

The T3.0 Plan conveys the approach by which NSA/CSS "rolls-up" numerous measures to support meaningful discussion and decisions, at the corporate level

- as it executes oversight of the larger combined effort of delivering the intent of the T3.0 vision.

Strategic Performance management of the T3.0 Initiative is focused on the 10 fundamental components of the T3.0 Initiative

Tactical goals & measures are focused on

Mission Mod Initiatives

Infrastructure Mod Initiatives

Workforce Mod Initiatives

Programmatic goals & measures, which support the modernization initiatives, are identified and retained at the PPAS element level

~~S//SI//REL~~

Summary

- Transformation 3.0 emphasizes, the integration [redacted] into every facet of NSA operations [redacted]
- Significant cryptologic benefits arise from integrating and exchanging information [redacted] among the UCS exploitation, defense, and warfare/attack systems
- The emerging challenges of the information age demand we:
  - Continue transformation of our mission capabilities, in the very process of acquisition and fielding
  - Build adequate capacity to absorb and support those transformational capabilities and
  - Employ a workforce that leads the pack in the information age

(b)(1)
(b)(3)-P.L. 86-36

~~S//SI//REL~~ 16

In a programmatic sense, T3.0 can be characterized as the convergence of three major, foundational initiatives to modernize and dramatically improve capabilities across the cryptologic enterprise.

-These initiatives are focused in **mission**, **infrastructure**, and **workforce**.

-All structured and managed to provide a seamless integration of E/D/eA

•Operating & integrating mission capabilities [redacted] provides tremendous Cryptologic advantages, **but** …

[redacted]

Comprehensive National Cybersecurity Initiative
Frequently Asked Questions

1. What is the "Cyber Initiative"?

~~(S//REL TO USA, FVEY)~~ The term "Cyber Initiative" is shorthand for the Comprehensive National Cybersecurity Initiative (CNCI), an initiative described in a Presidential Directive, NSPD-54/HSPD-23 aimed at increasing our Nation's security in cyberspace, and particularly providing substantially improved security for our federal networks and information systems. The initiative, developed by a cross-governmental group of more than 22 Federal departments and agencies, provides an enduring and comprehensive national approach to cyber security in which NSA plays a key role.

2. What is the problem that resulted in the creation of the CNCI?

(U//~~FOUO~~) The U.S. information infrastructure – including telecommunications and computer networks and systems, and the data that reside on them – is critical to virtually every aspect of modern life. Unfortunately, the interconnection of telecommunications and information networks that underlies our way of life creates vulnerabilities that hostile actors are exploiting every day. Systems that once operated only in isolation now function as part of global information networks, while consumers continually demand more capabilities in fewer, smaller and more portable devices. At the same time, much of the design, manufacture, and service of information technology has moved overseas. As government, private sector, and personal activities continue to move to networked operations, as our digital systems add ever more capabilities, and as wireless systems become even more ubiquitous, our vulnerabilities will only continue to grow.

(U//~~FOUO~~) While the United States has not been physically attacked on our homeland since 9/11, U.S. Government information systems face virtually constant intrusion attempts. Our information infrastructure – including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries – increasingly is being targeted for exploitation, disruption, and destruction by a growing array of state and non-state adversaries.

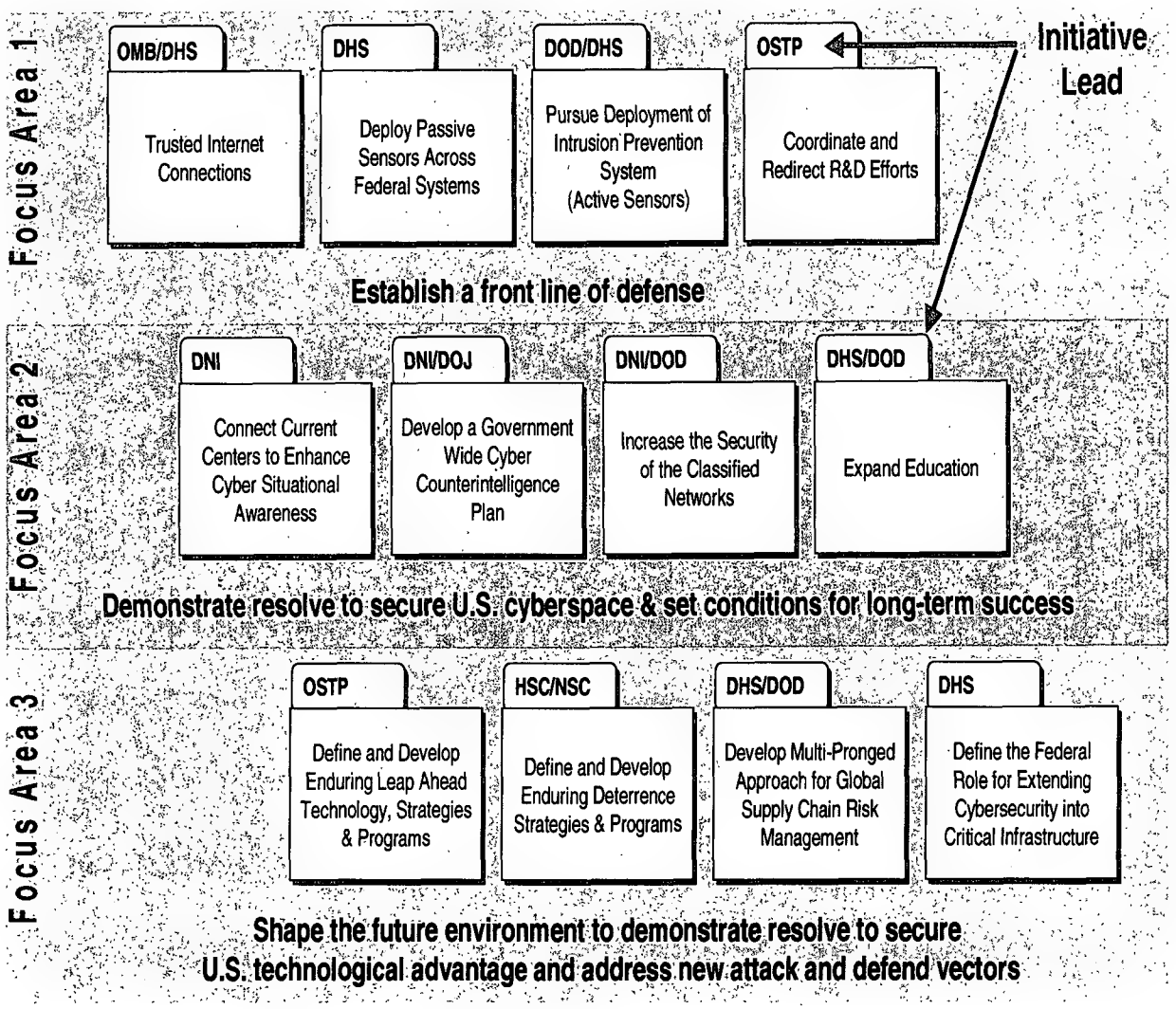
3. How does the CNCI address this threat?

~~(S//REL TO USA, FVEY)~~ The CNCI addresses this threat through an interagency effort to develop and implement 12 interdependent initiatives (see Figure 1) and seven enabling strategic activities (see Figure 2). The initiatives will close identified cybersecurity gaps. Strategic enablers are critical to providing the foundational capabilities to support these initiatives. The Director of National Intelligence (DNI) has the responsibility of ensuring that Departments and agencies implement these initiatives and enablers as planned.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

~~SECRET//REL TO USA, FVEY~~

(U//~~FOUO~~) The 12 Interdependent Cybersecurity Initiatives


Initiative Lead
Focus Area 1
OMB/DHS
Trusted Internet Connections
DHS
Deploy Passive Sensors Across Federal Systems
DOD/DHS
Pursue Deployment of Intrusion Prevention System (Active Sensors)
OSTP
Coordinate and Redirect R&D Efforts
Establish a front line of defense
Focus Area 2
DNI
Connect Current Centers to Enhance Cyber Situational Awareness
DNI/DOJ
Develop a Government Wide Cyber Counterintelligence Plan
DNI/DOD
Increase the Security of the Classified Networks
DHS/DOD
Expand Education
Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success
Focus Area 3
OSTP
Define and Develop Enduring Leap Ahead Technology, Strategies & Programs
HSC/NSC
Define and Develop Enduring Deterrence Strategies & Programs
DHS/DOD
Develop Multi-Pronged Approach for Global Supply Chain Risk Management
DHS
Define the Federal Role for Extending Cybersecurity into Critical Infrastructure
Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors

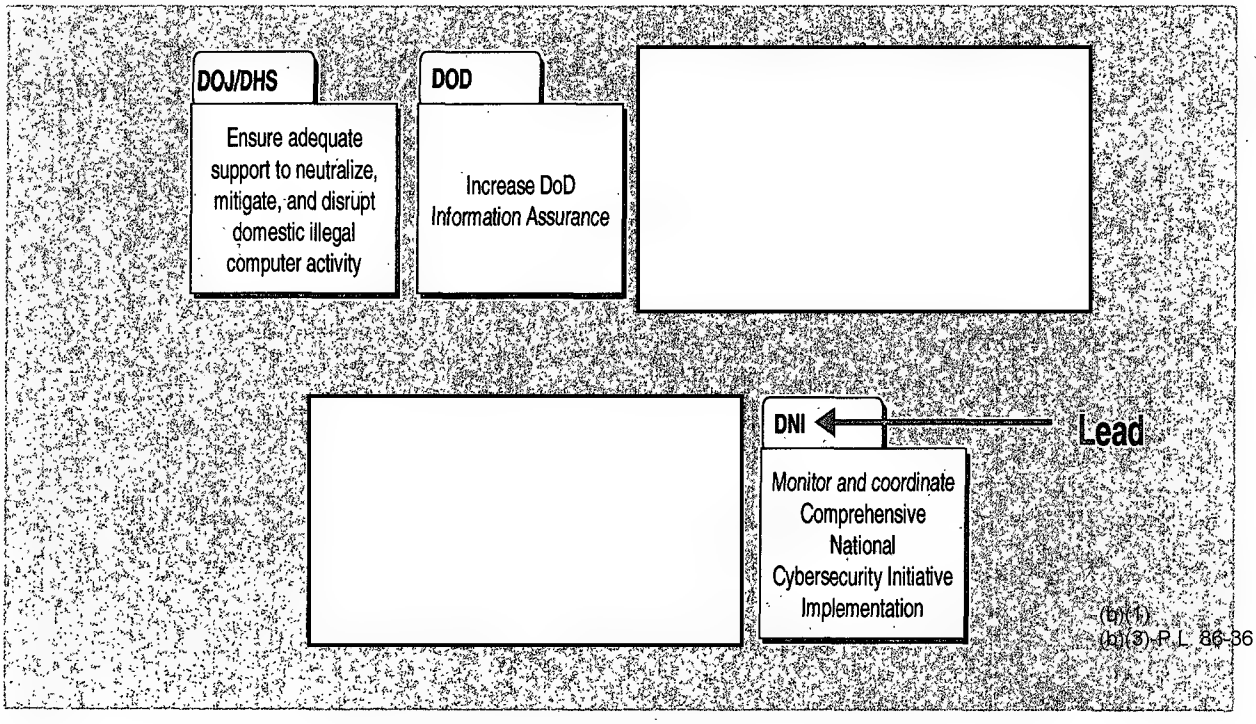
~~SECRET//REL TO USA, FVEY~~

Figure 1: The 12 Interdependent Cybersecurity Initiatives (U)

~~SECRET//REL TO USA, FVEY~~

(~~U//FOUO~~) ~~The~~ 7 Interdependent Strategic Enablers

The Comprehensive National Cybersecurity Initiative includes seven priority areas for investment that are essential to enable the activities to defend U.S. networks:


DOJ/DHS
Ensure adequate support to neutralize, mitigate, and disrupt domestic illegal computer activity
DOD
Increase DoD Information Assurance
DNI
Lead
Monitor and coordinate Comprehensive National Cybersecurity Initiative Implementation

(b)(1)
(b)(3)-P.L. 86-36

The Comprehensive National Cybersecurity Initiative is pulling together a full spectrum view from across all the USG mission areas, to include law enforcement, intelligence, military, diplomatic and homeland security.

~~SECRET//REL TO USA, FVEY~~

Figure 2: The 7 Interdependent Strategic Enablers (U)

NSA/CSS has multiple deliverables associated with the CNCI. Of the 12 initiatives and seven enablers pictured above, NSA participation

(b)(3)-P.L. 8

(U//~~FOUO~~) CI Initiative 3: Deploy Intrusion Prevention System (Active Sensors) across the Federal Systems Enterprise

(b)(1)
(b)(3)-P.L. 8

(b)(3)-P.L. 8

(U//~~FOUO~~) CI Initiative 8: Expand Cyber Education

~~(C//REL USA, FVEY)~~ NSA/CSS already partners extensively with the Services to ensure the cryptologic workforce has the skills to meet current and future CNO challenges.

(b)(3)-P.L. 8

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Enabler E:

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(U//~~FOUO~~) Enabler F: [redacted] (b)(3)-P.L. 86-36

[redacted]

4. Are all the initiatives/enablers equally important? (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

[redacted]

5. What role did NSA/CSS play in helping formulate the CNCI?

~~(TS//REL TO USA, FVEY)~~ The CNCI was developed over many months at the direction of the President, in a process led by the Director of National Intelligence and overseen by his Homeland and National Security Advisors. Important contributions were made by 22 Intelligence Agencies in what has become the largest cross-government effort in recent history. [redacted]

[redacted] (b)(3)-P.L. 8

6. How will the missions or work of NSA/CSS change under the CNCI?

~~(TS//SI//REL USA, FVEY)~~ During the development of the CNCI, it became clear to all participants that the cryptologic system forms much of the technical foundation of an effective strategy to secure cyberspace. All of our responsibilities under the CNCI are within our *existing* authorities and missions, i.e., SIGINT, Information Assurance, enabling network warfare under JFCC-NW, and providing technical assistance to other federal agencies. The vast majority of our work under the CNCI is work we are already doing under our Transformation 3.0. [redacted]

[redacted]

 (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

[redacted]

~~(TS//REL TO USA, FVEY)~~ With our existing authorities as part of DoD and the Intelligence Community, [redacted] (b)(3)-P.L. 86-36 [redacted] we will make contributions to the Nation's cybersecurity in ways that no one else can:

[redacted]

- **Information Assurance** -- We know the vulnerabilities and will accelerate and expand our efforts to secure National Security Systems and will continue to make our expertise available to other agencies in the federal government as appropriate.

[redacted]

- **Technical Assistance and Support** -- Each day, we provide technical assistance and support to other federal agencies, and this initiative will be no different. We'll

[redacted]

7. Will we get additional funding or personnel under the CNCI?

~~(TS//REL TO USA, FVEY)~~ Yes, if Congress approves the President's budget, NSA will receive additional funding and personnel to execute our roles in this initiative. While this specific information cannot be posted on the website, you can obtain these details, as appropriate, through your organization's leadership.

8. Is what we've heard about the Cyber Initiative in the press accurate?

9. What is the way ahead for NSA in the CNCI?

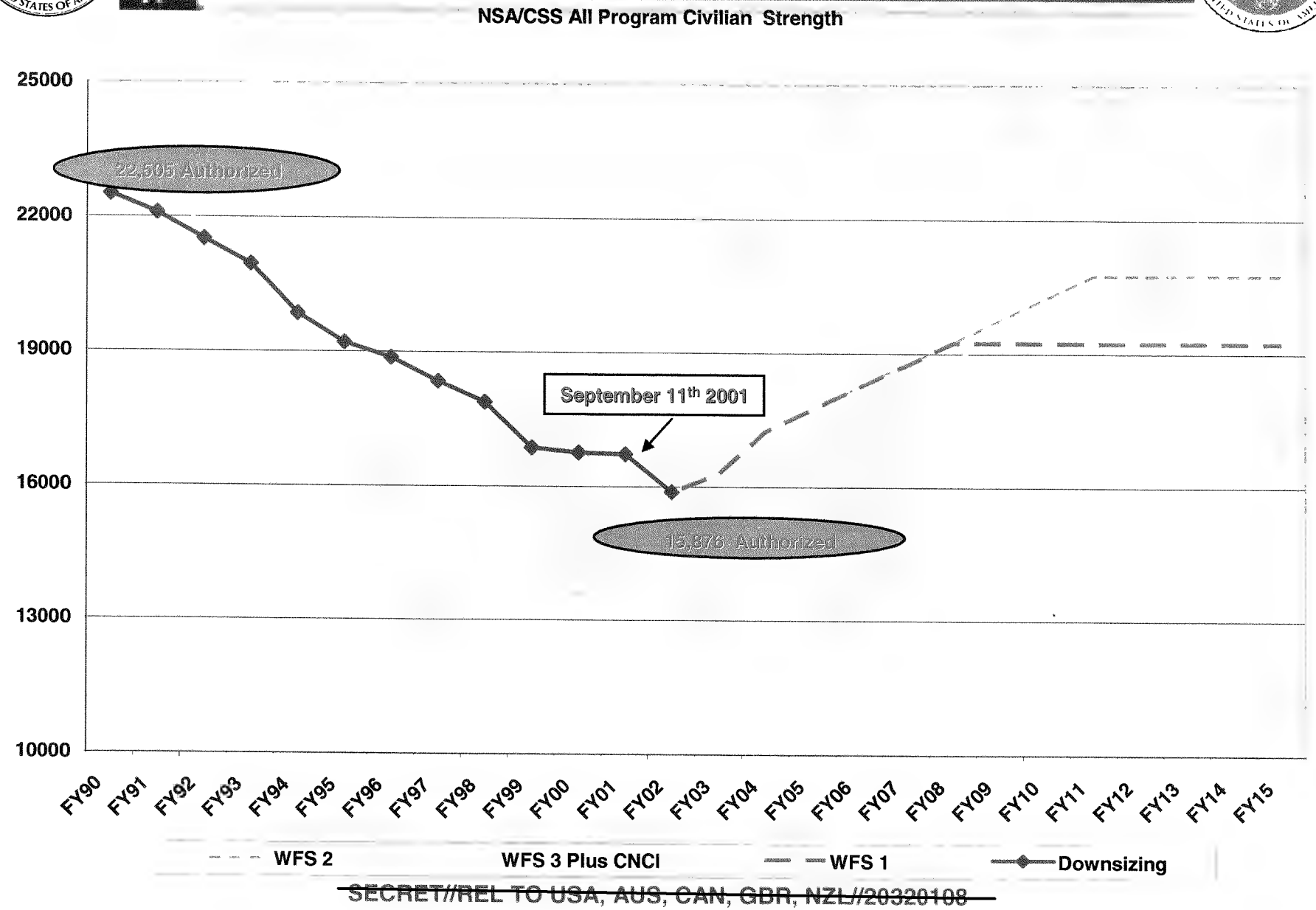
(b)(1)
(b)(3)-P.L. 86-36

HR

State of the Workforce

October 2008

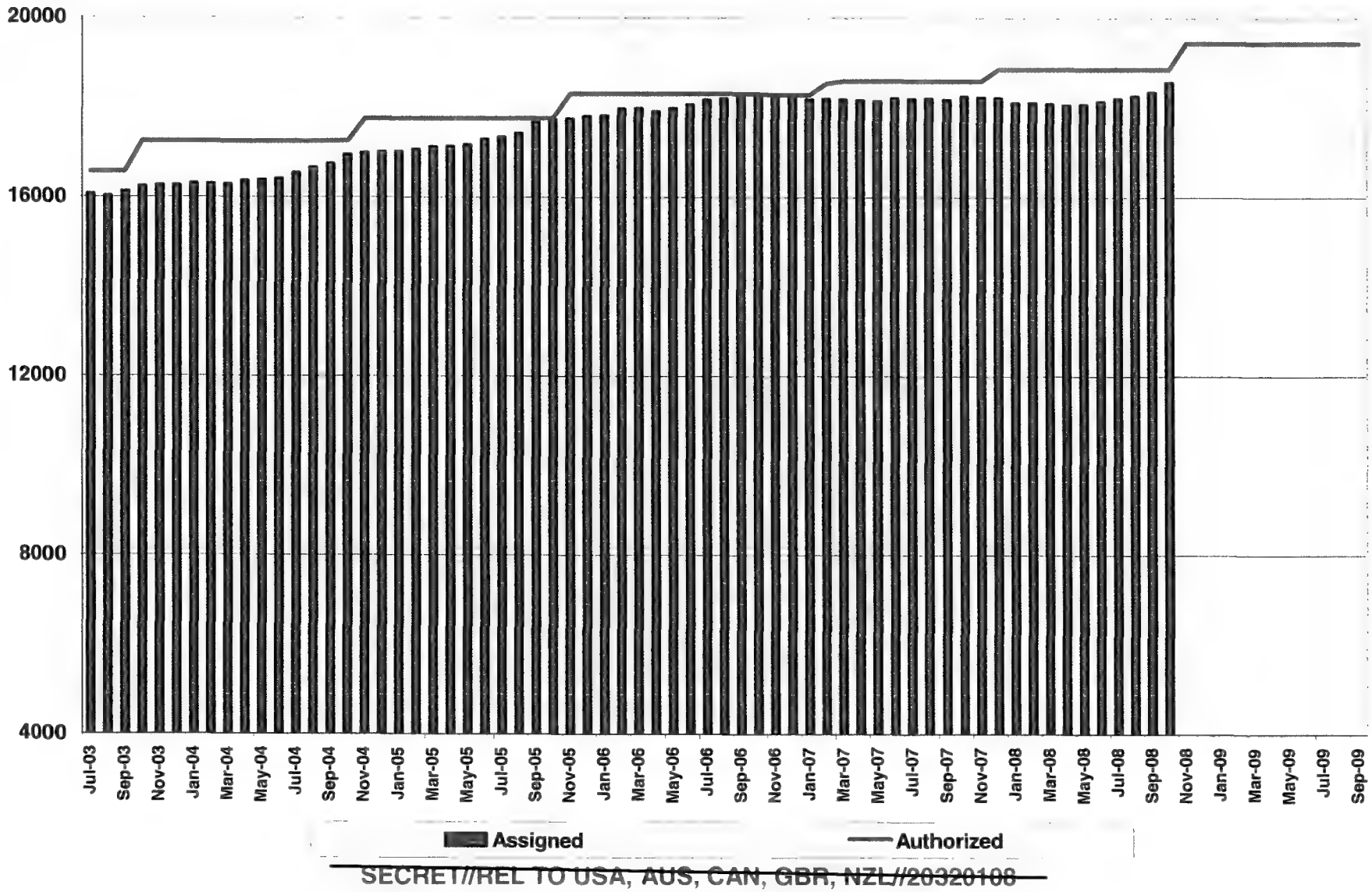
Civilian Workforce Strategy in Context



~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

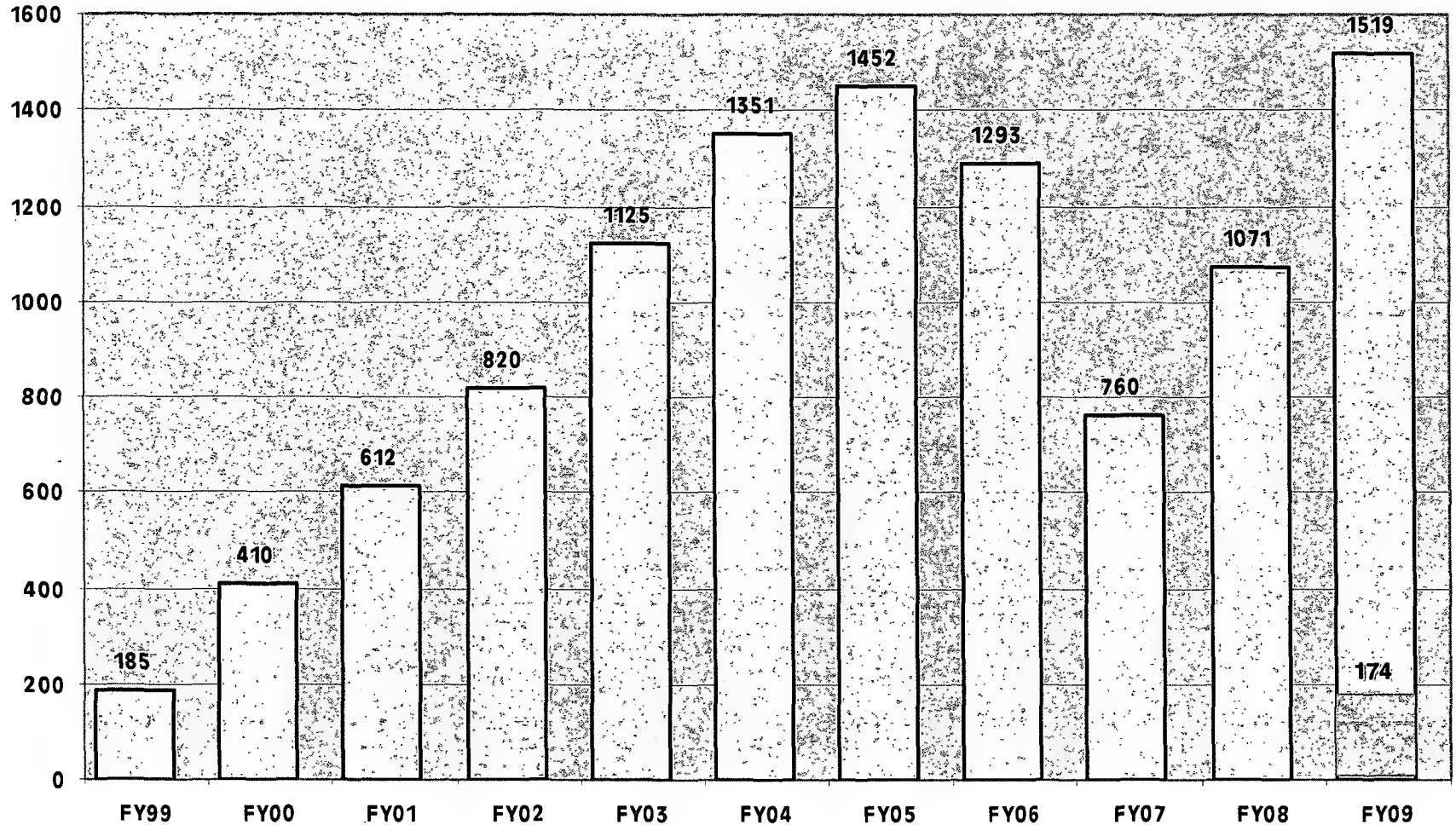
Civilian Workforce Strategy in Context

Overall Authorized vs. Assigned FY04-FY09

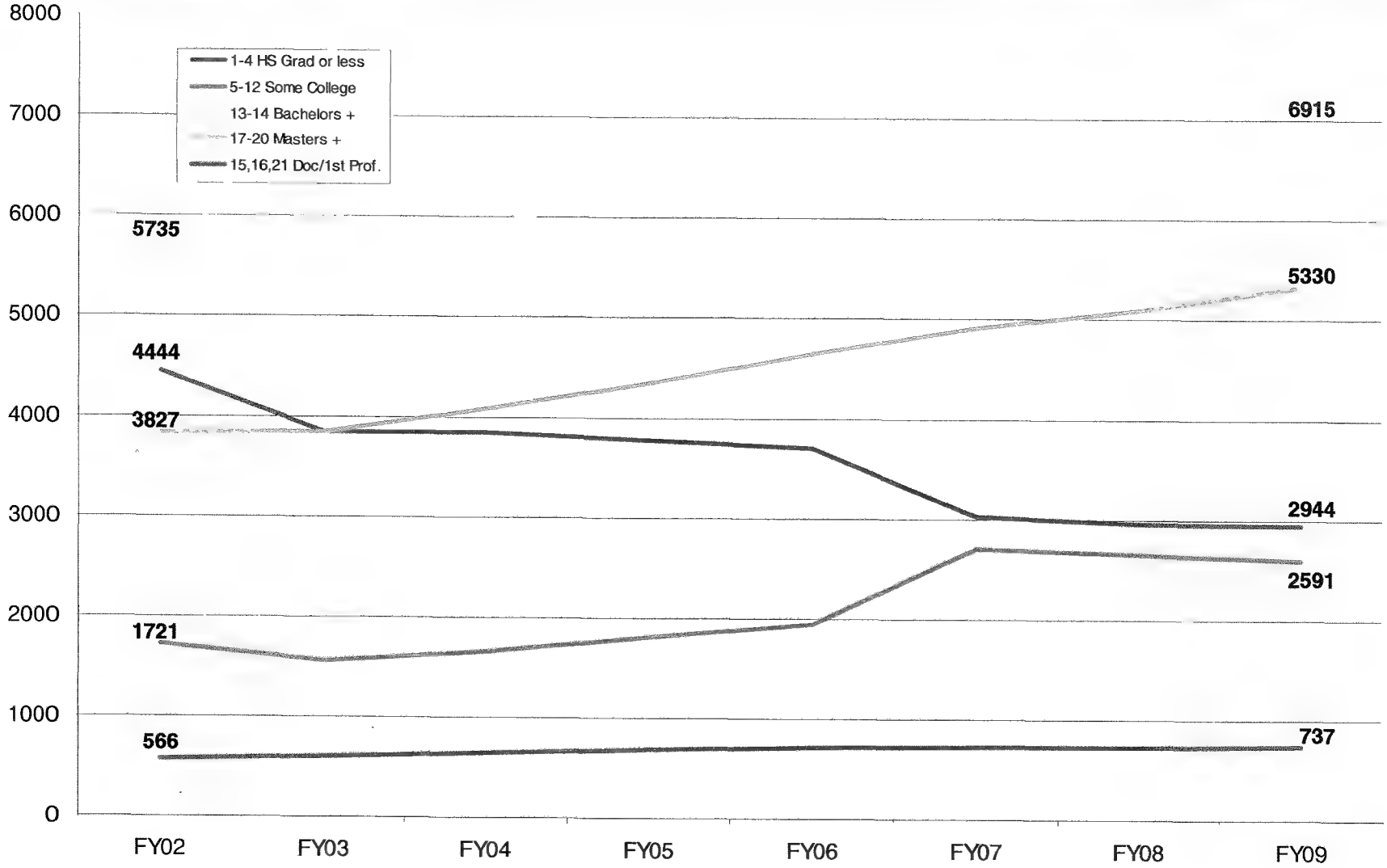


FY99 through FY09 Hiring Programs

FY99 - FY09 Hiring Programs (Permanent/FTA)

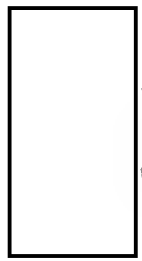


Education Levels Start FY02 – Start FY09



Civilian Population Change Start FY02 – Start FY09

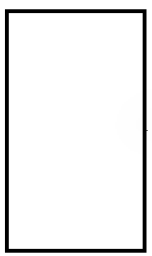
Start FY02 Population
(16124 – *FTE/All Hire Types)*



Analytic and Technical
Security
Acq & Business
OL&M and Support
All Other

(b)(1)
(b)(3)-P.L. 86-36

Start FY09 Population
(18569 – *FTE/All Hire Types*)



Analytic and Technical
Security
Acq & Business
OL&M and Support
All Other

National Security Agency/ Central Security Service

Civilian Employment Plan
FY 2008

19 October 2007

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Table of Contents

This Table of Contents is Unclassified

		Page
1.	Introduction	3
	A. Mission and Vision	3
	B. NSA's Organization	4
	C. Overview	6
	D. Historical Perspectives	8
	E. The Planning Environment	9
	F. IT Linkage	12
	G. Facilities as a Key Enabler	13
	H. Transformation 3.0	14
	I. FY 2009-FY 2013 Program Build	19
2.	What It All Means	19
	A. Focus Areas	19
	1. The Nation Expects a High Level of Competence	20
	2. Collaboration Produces the Best Results	21
	3. Agile and Responsive to Dynamic Needs	22
	B. Identifying Requisite Competencies	23
	C. Implementation	24
	1. Workforce Development	25
	2. Staffing/Succession Planning	26
	3. Retention and Attrition Management	27
	4. Workforce Performance Management	28
	5. Recruiting and Hiring	28
	6. Occupational Health, Environment, and Safety	28
3.	Civilian Workforce Profiles	29

1. (U) Introduction -- Civilian Employment Plan for the National Security Agency

(U) This Civilian Employment Plan (CEP) provides an overview of the dynamics and imperatives shaping and "driving" the NSA workforce. It explains who we are and what we do; describes changes in staffing levels and skills mix in response to changes in agency and national intelligence missions; and provides plans for hiring, development and retention to accommodate changes in mission duties and jobs, fill vacancies, and replace losses. In synergistic harmony with our Workforce Strategy 3.0 "Building the Future Workforce," our Human Capital Implementation Plan, our Facilities Strategic Plan and our Enterprise Information Technology Master Plan, it rounds out a full suite of deliberate planning and the concomitant documentation designed to assist the Agency in optimizing and leveraging its uniquely talented workforce to meet mission ends.

A. (U) Mission and Vision

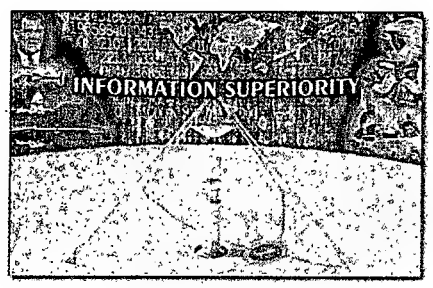
(U) NSA's mission is to deliver responsive, reliable, effective, and expert Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enable Network Warfare operations to gain a decisive information advantage for the Nation and our allies under all circumstances.

Our Vision is **Global Cryptologic Dominance through National Network Advantage.**

To achieve this Vision, NSA/CSS will:

- Dominate global cryptology
- Secure national security systems
- Connect people, sensors, systems, and information on a global scale
- And, leverage our unique relationships with government, industry, academia, and foreign partners

(U) The National Security Agency exists to provide our nation the information superiority it requires.



(U) Intelligence and information systems security have always complemented each other. Intelligence gives us an information advantage over our adversaries and competitors, and information systems security prevents others from gaining a comparable advantage over us. In today's environment, the two functions serve as the offensive and defensive squads of a team dedicated to a single goal - information superiority for America and its Allies.

(U) In order to fulfill multiple cryptologic roles across the globe, NSA relies heavily on the five uniformed services for support. These Service Cryptologic Elements (SCEs) make up what is known as the Central Security Service (CSS) with DIRNSA as its chief.

(U//~~FOUO~~) The National Security Agency/Central Security Service (NSA/CSS) conducts the two core missions of the United States Cryptologic System (USCS): SIGINT and IA. NSA exploits the signals of foreign targets around the globe for the purposes of providing foreign intelligence and counterintelligence information, as well as to support military operations. The cryptologic effort comes full circle as NSA [redacted] to help secure classified national security and sensitive U.S. government information systems.

(U) Today, we operate within a complex information technology (IT) environment characterized by expanding global networks, increasing volumes of data, and rapidly changing technologies, placing greater challenges and demands on our SIGINT and IA missions. Moreover, the Internet and e-commerce arenas are facilitating the use of commercial off-the-shelf (COTS) applications and increasing the need for both IT expertise and systems security.

(U) All of the people and the resources of the National Security Agency are focused on providing Information Superiority for our nation and its allies. Information superiority assures that the United States will be able to store, process, and disseminate an uninterrupted flow of information while denying an adversary the ability to do the same.

B. (U) NSA's Organization

(U) Understanding NSA/CSS's organization is key to understanding the approach we are taking to our workforce strategy. NSA is organized around five line directorates, which include Signals Intelligence, Information Assurance, Technology, Research, and Foreign Affairs. Additionally, NSA has two major mission areas that are aligned under the DIRNSA, the Central Security Service and Joint Functional Component Command, Network Warfare. These line organizations are supported by staff offices and enabler organizations, as shown in Chart 1. Additionally, the DIRNSA "wears three hats" on a daily basis – first, he is the Director of NSA (a Combat Support Agency under the Department of Defense); second, he is the Commander, Central Security Service/Joint Functional Component Command, Network Warfare (as a component commander under United States Strategic Command); and third, he is the Director, United States Security Service (as the federal government's executive agent for information assurance). DIRNSA fulfills all these duties simultaneously, while also serving as one of the senior members of the United States Intelligence Community.

Unclassified

(U~~//FOUO)~~ NSA also has a worldwide mission, with over [redacted]

[redacted]

(b)(3)-P.L. 86-36

[redacted]

17

C. (U) Overview

In the performance of its multiple missions over the years, we have excelled for many reasons, not the least of which has been a continuing commitment to acquiring and building a workforce of tremendous skill and dedication.

(U~~//FOUO)~~ As the Information Age continues to unfold, however, we find it increasingly unmanageable to keep up with the volume, velocity, and variety of information handled by modern communications systems. (b)(1) (b)(3)-P.L. 86-36 Cyberspace has emerged as a major theater of conflict –

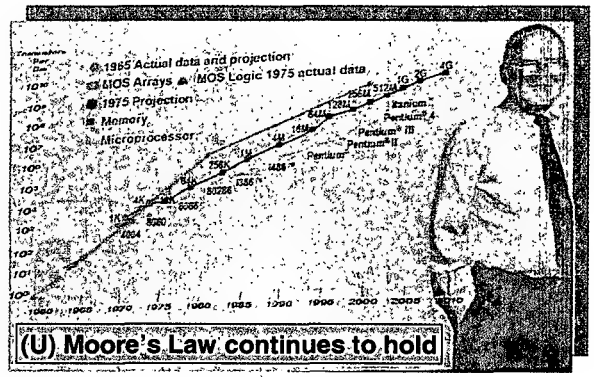
(b)(3)-P.L. 86-36

(U) Data and functions that are critical to the nation's security are increasingly consigned to systems that are too complex and fluid for all vulnerabilities to be found, much less eliminated. Commercial technologies, often built by unvetted sources to uncertain national security standards, play a growing role in these systems. They reside across networks our Nation and our military depend upon, expanding the number of points where a breach can occur and the number of points that a breach can compromise.

(U) This fusion of commonality, dependence and technological advance presents difficult and unprecedented challenges. We must keep pace with dynamic changes in global telecommunications while simultaneously defeating daily attacks launched on a global scale though the uncontrolled media of global networks. We must also do this while conducting high tempo operations (which surged after 9/11 and show no signs of abating). Our workforce faces an immense challenge, i.e., to master the enabling technologies of the Information Age while operating within an environment of intense and constant change. Our answer (Transformation 3.0) to this complex and difficult situation involves our transforming [redacted] establishing a collaborative real-time system of people, processes and technologies to achieve NSA/CSS's vision of global cryptologic dominance.

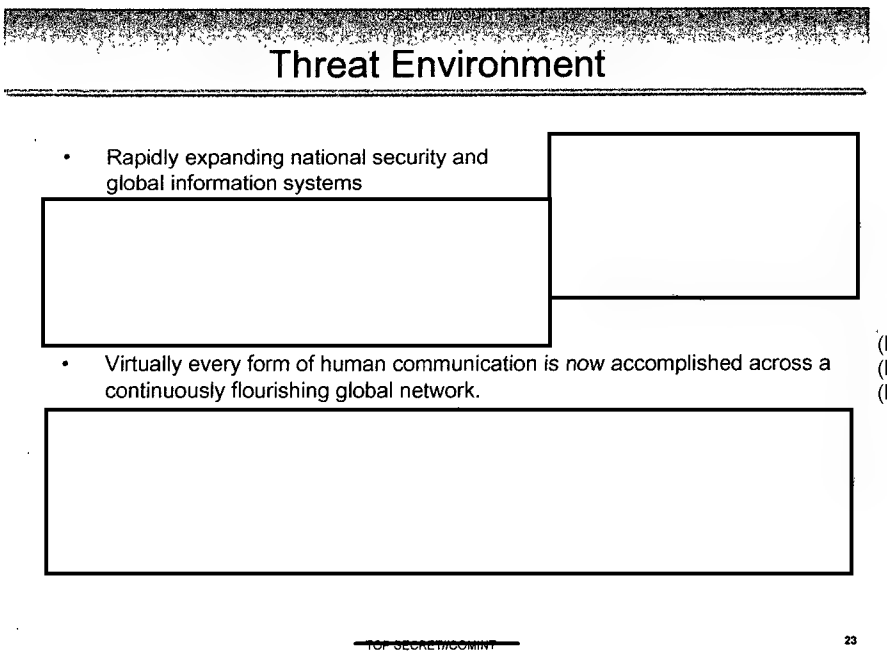
(U) Moore's Law continues to hold, with processors doubling in speed every 12-24 months (as they have since 1965). Nanotech manufacturing techniques are the latest

surge in the global semiconductor industry, driving annual revenues towards a quarter of a trillion dollars. The Internet is also surging. Users have tripled in the past seven years; 1.1 billion accounts now send almost 100 billion emails a day. These users are evolving the Internet into a grid, with practically all transmissions using some part of its infrastructure. A greater percentage of these transmissions are mobile, involving wireless nodes and the two billion (and climbing) cellular phones in use. Over all, global networks now carry petabytes (10^{15}) of information every day – data equivalent to the total printed output of humankind since the birth of history. Despite occasional financial shocks, these technologies continue to advance at remarkable speeds. In fact, their pace of change may be accelerating as they feed upon each other to drive even shorter development cycles.



(U) Moore's Law continues to hold

(b)(1)
(b)(3)-P.L. 86-36


TOP SECRET//COMINT
Threat Environment
• Rapidly expanding national security and global information systems
• Virtually every form of human communication is now accomplished across a continuously flourishing global network.
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
TOP SECRET//COMINT
23

(U//~~FOUO~~) Understandably, these unique, dynamic and rapidly evolving conditions place unprecedented and unmatched demands on our workforce. The deliberate and dedicated workforce strategies that NSA has developed pursue long-term and comprehensive solutions to complex challenges through development, nurturing and sustainment of a world-class employee base. Further, our strategies recognize that the traditional, one-dimensional workforce of the past is now gone. Our talented workforce of the future will be more diverse, more flexible, more fluid, and will be a mix of the three components (civilian, military, and contractor) harmonized to optimize the distinct attributes of all employees.

D. (U) Historical Perspectives

(U~~//FOUO)~~ These serious threats and the ever increasing pace of technological change present unique challenges to our current leadership but one fact remains certain - **our people are our greatest asset for meeting these challenges.** For years, our strategic planning documents have been filled with recognition of that fact. From the 1993 Workforce in Transition Task Force Report (prepared in the midst of a decade of downsizing) that stated, "NSA must change the ... management of its most critical ...asset – the work force..." to the post-9/11 Work Force Strategy (formed at the beginning of the Agency's latest growth cycle) which recognized that "People and the knowledge they possess are the heart of the NSA/CSS," Agency leaders have asserted that it is the highly-skilled, dedicated men and women of our workforce who ensure our success. More than a decade ago, NSA recognized the need to develop far-sighted and comprehensive management of its workforce in light of what was then termed "challenges which are without precedent." As a result, Agency leadership developed

(b)(1)
(b)(3)-P.L. 86-36

and endorsed a series of future-focused work force plans that guided downsizing through the 1990's and governed growth starting in FY2003. These efforts bore significant benefits to the national intelligence community over the past fifteen years as they resulted in the identification of the critical skills needed for current and future success. In addition, they helped the Agency shape programs to protect the key areas that provided a platform to build on after the 9/11 attacks. As a result, we have been able to provide support across many fronts, push more Expeditionary Cryptologists to the front lines of the war on terror, and have a direct hand in some

[redacted]

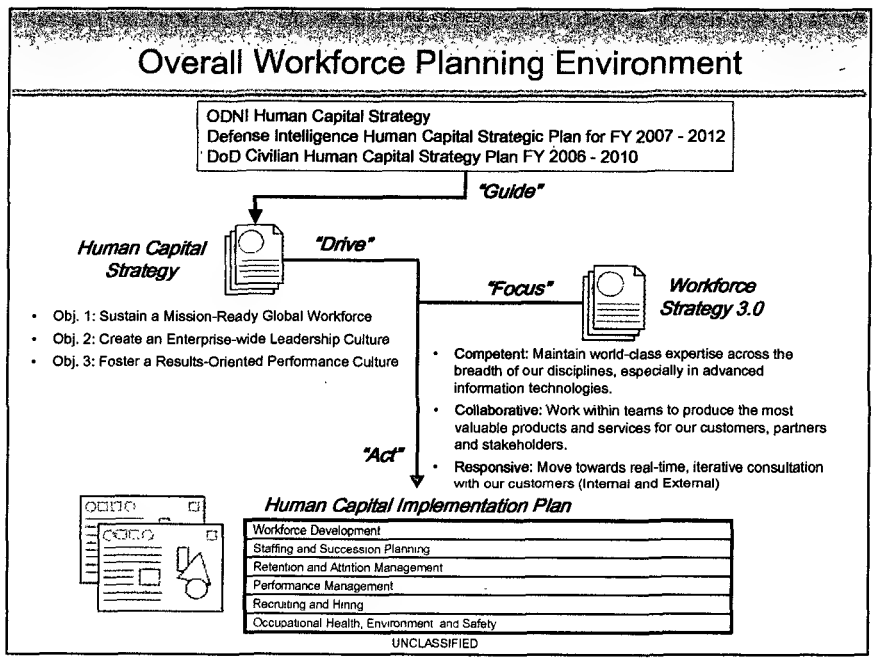
[redacted]

E. (U) The Planning Environment

(b)(3)-P.L. 86-36

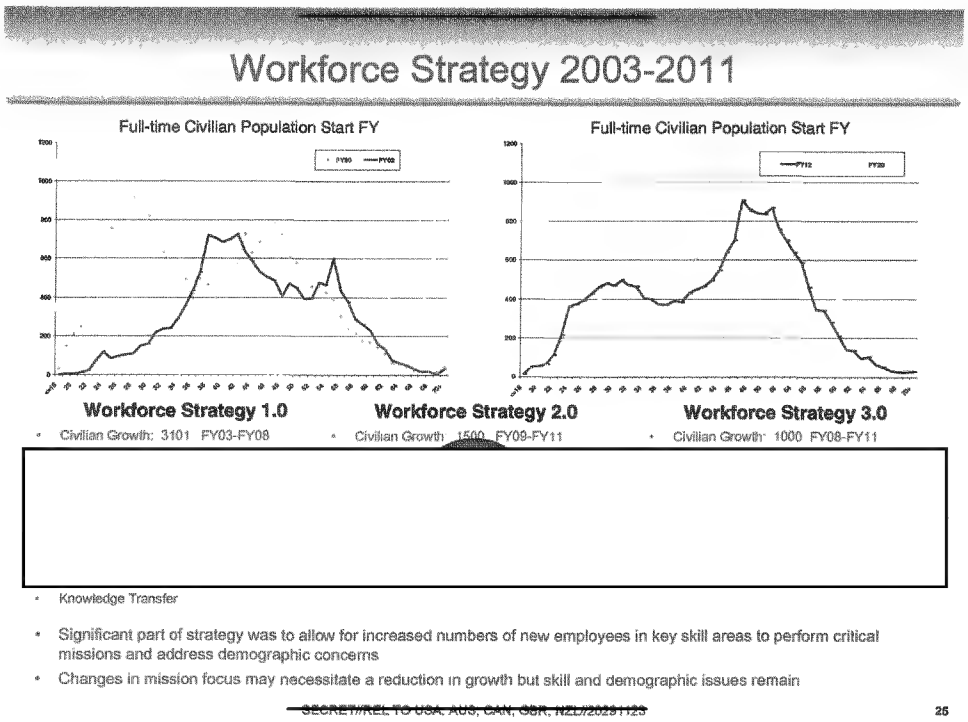
(U//~~FOUO~~) To assure our work force planning efforts are not conducted "in a vacuum," NSA has intentionally and deliberately included workforce strategy and issues as key components of the overall agency and program strategy. To that end we built and are constantly refining a Human Capital (HC) management system/structure that is designed to attract, retain, develop, enable, and deploy a mission-ready global workforce, inspired and guided by leaders at all levels, to deliver extraordinary results. NSA/CSS strongly believes that HC initiatives can and do play a key role in transforming organizational ethos and can have a dramatic, positive effect on the Agency's ability to achieve its critical national security mission goals and objectives.

(U//~~FOUO~~) The Agency's Human Capital Strategy is aligned with overarching strategic planning initiatives of the Department of Defense (DoD) and the Office of the Director of National Intelligence (ODNI), is in consonance with the other strategic initiatives underway in the Agency, and provides our blueprint for ensuring the diverse, highly skilled workforce needed to accomplish the Agency's mission. It outlines a comprehensive approach for achieving proper skills alignment, developing employee competencies to optimize their ability to contribute to the mission, honing leadership skills, and instilling/implementing a performance-based culture. The HC Strategy supports all four of the NSA/CSS Strategic Plan goals: Mission; Transformation; People; and Business Practices.


Overall Workforce Planning Environment
ODNI Human Capital Strategy
Defense Intelligence Human Capital Strategic Plan for FY 2007 - 2012
DoD Civilian Human Capital Strategy Plan FY 2006 - 2010
"Guide"
Human Capital Strategy
"Drive"
"Focus"
Workforce Strategy 3.0
Obj. 1: Sustain a Mission-Ready Global Workforce
Obj. 2: Create an Enterprise-wide Leadership Culture
Obj. 3: Foster a Results-Oriented Performance Culture
Competent: Maintain world-class expertise across the breadth of our disciplines, especially in advanced information technologies.
Collaborative: Work within teams to produce the most valuable products and services for our customers, partners and stakeholders.
Responsive: Move towards real-time, iterative consultation with our customers (Internal and External)
"Act"
Human Capital Implementation Plan
Workforce Development
Staffing and Succession Planning
Retention and Attrition Management
Performance Management
Recruiting and Hiring
Occupational Health, Environment and Safety
UNCLASSIFIED

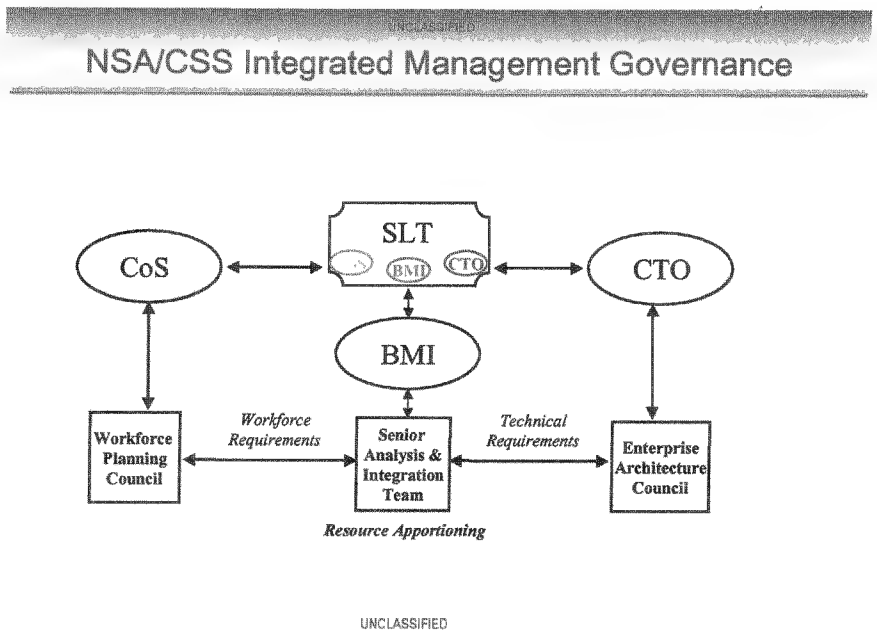
(U) Workforce Strategy 3.0 attempts to answer: *"What skills will NSA/CSS emphasize in our workforce recruiting, retention and development programs?"* This answer will guide our workforce planning decisions over the next three years (FY08-10). It will take into account our constantly changing operating environment and the resulting imperative for a responsive, collaborative and highly competent workforce. In building the future workforce, we specifically focus on improving our capabilities to: forecast and assess staffing, skill and competency needs; attract, hire, reward, develop and deploy our employees to ensure the agility and readiness the mission demands; and design and institutionalize Human Capital programs that facilitate/enhance teaming and collaboration as well as sharing across the Intelligence Community (IC).

(U) The Human Capital Implementation Plan is based on both the Human Capital Strategy and Workforce Strategy 3.0. It provides specific Agency-level guidance by Human Capital functional area. Senior leadership will use this Implementation Plan to approve both the FY08 Hiring Plan and the FY08 Promotion Program. Each designated Human Capital area lead will work with mission elements and NSA/CSS Skill Community staffs to identify sub-activities and individual milestones, develop schedules and performance measures, and document and track progress.


Workforce Strategy 2003-2011
Full-time Civilian Population Start FY
Full-time Civilian Population Start FY
Workforce Strategy 1.0
Civilian Growth: 3101 FY03-FY08
Workforce Strategy 2.0
Civilian Growth: 1500 FY09-FY11
Workforce Strategy 3.0
Civilian Growth: 1000 FY08-FY11
Knowledge Transfer
Significant part of strategy was to allow for increased numbers of new employees in key skill areas to perform critical missions and address demographic concerns
Changes in mission focus may necessitate a reduction in growth but skill and demographic issues remain
~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~
25

(b)(1)
(b)(3)-P.L.

(U) To further reinforce the critical nature of workforce planning activities and to ensure they are coordinated and integrated with other Agency plans and processes, the Senior Leadership Team (SLT) recently approved the stand up of the Workforce Planning Council.



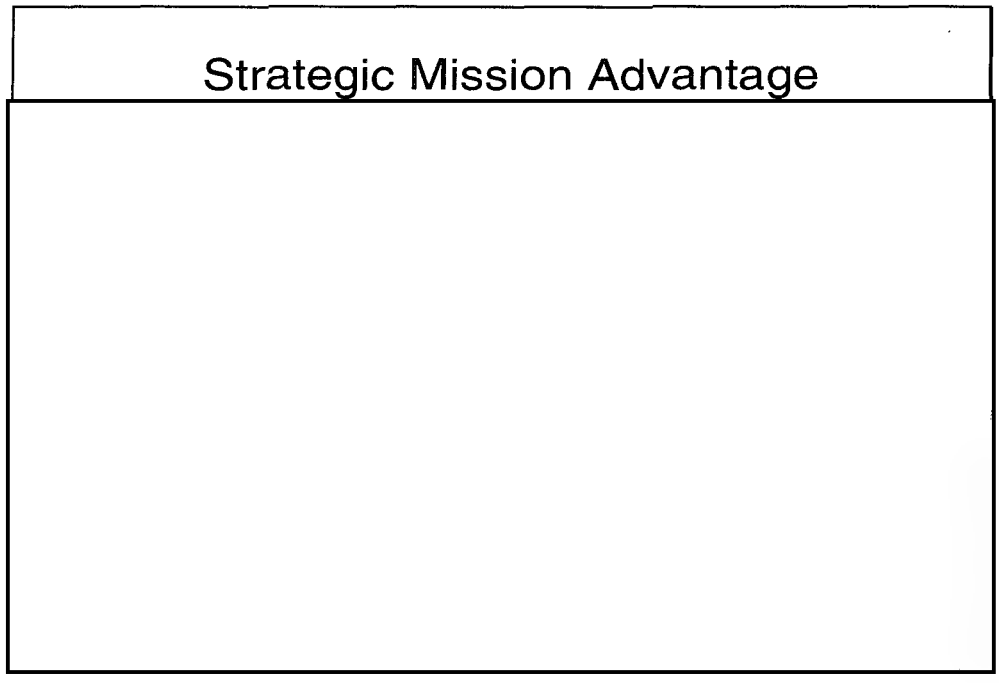
This body, chaired by the Chief of Staff, will work with the SLT, the Senior Analysis and Integration Team (SAIT), Business Management Integration, the Chief Technology Officer and the Enterprise Architecture Council within an integrated management framework to apportion, balance and align resources to maximum effect.

(U//~~FOUO~~) Within this deliberate planning context, we are pleased to offer that this Civilian Employment Plan effort is a continuation of NSA's on-going workforce strategic planning efforts, and we are also pleased to be able to tangibly contribute to an overall DNI effort on behalf of the entire Intelligence Community.

F: (U) IT Linkage

~~(S//SI)~~ Understandably, in a globally engaged, cutting edge activity like NSA/CSS, we have to leverage and optimize technology at every opportunity – both to our advantage and to disadvantage those who would do our nation harm. In two venues, in corporate IT and in the platforms and facilities in which our workforce operates, NSA/CSS clearly recognizes that these become the very tools of the trade for our uniquely talented workforce. As a result, in regards to the first venue, we seek to leverage technology, especially the IT spectrum, as the Agency's Strategic Mission Advantage. We expect that modernizing NSA/CSS' Enterprise Information Technology (EIT) has a ripple effect that, coupled with the success of Transformation 3.0, Workforce Strategy 3.0, cryptanalysis, and other mission applications, will ultimately lead to the United States' (US) information dominance. Through the modernization of our EIT, we will supply our mission elements and equip our people with the speed, agility, interoperability, convergence, reliability, and availability they need to be successful. A modernized IT Infrastructure (ITI) enables

(b)(1)
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-P.L. 86-36

G. (U) Facilities as a Key Enabler

(U//~~FOUO~~) Much as being done in the IT arena to better enhance Agency capabilities and enable the workforce, NSA/CSS has taken a similar deliberate approach to its facilities as key platforms for effective operations. To this end, NSA/CSS complements its other deliberate planning documents with a Facilities Strategic Plan which represents the Agency's strategic vision, goals and plans for its facilities infrastructure in support of mission and Information Technology (IT) systems. This vision began with the construction of the Agency's Cryptologic Centers and is intended to outline the requirements and planning necessary to improve the existing infrastructure and provide for future mission and IT growth. As stated in an October 2006 business case, the phrase, "Power, Space and Cooling" is an overarching label for the basic ingredients needed to operate the IT and mission assets at the National Security Agency (NSA), including the ability to optimize a uniquely talented workforce with the best and latest tools. Power, Space and Cooling (PSC) supports mission modernization and IT Modernization at NSAW and across the extended enterprise by increasing both the power capacity and reliability while sustaining the existing infrastructure and reducing the backlog of maintenance and repair. Again, this plan is developed and implemented as a key part of an overall strategic resourcing approach to the Agency's challenges.

(U//~~FOUO~~) In order to successfully deliver the PSC solution and to ensure that Transformation 3.0 is fully supported and realized, NSA/CSS recognizes it must have the ability to increase its workforce in key functions (such as power engineers and project managers) to help manage the PSC program. To accomplish this, personnel with

technical, planning and integration skills will have to be acquired to complement the already knowledgeable workforce in the Installations and Logistics (I&L) arena.

H. (U) Transformation 3.0

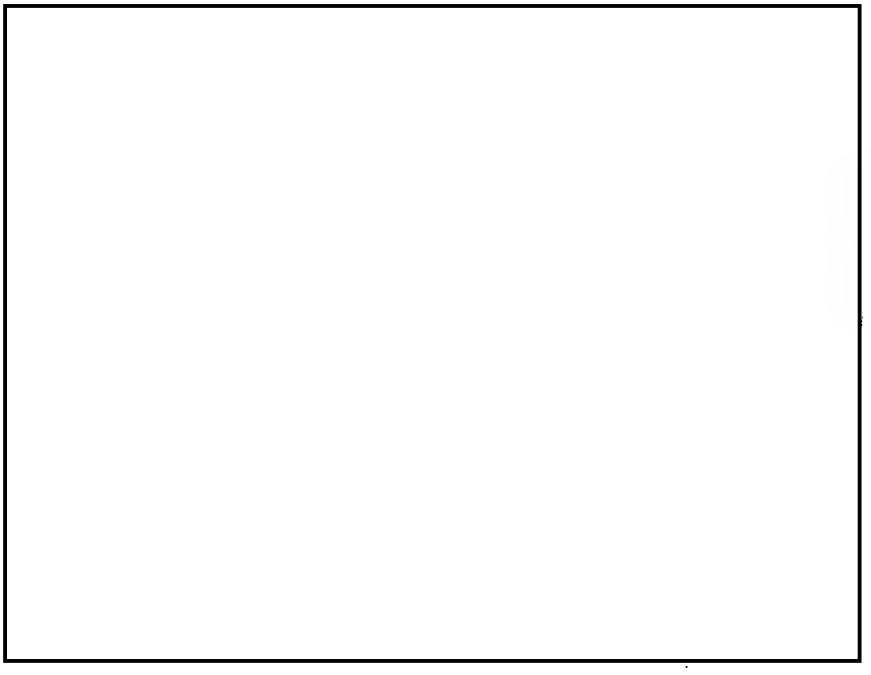
(U) As discussion of workforce issues in NSA could not take place without framing it in the context of our Agency-wide Transformation initiative. In developing this sweeping initiative, the Agency recognized that a key attribute must be a major rethinking about how we employ and leverage our infinitely talented and valuable workforce. As Transformation has been approached in NSA/CSS, its progression within NSA/CSS spans three discrete stages.

- (U) T1.0 – **Modernization** – Following the cold war, T1.0 improved corporate business processes, shaped the workforce, modernized technology, and updated operations – better positioning the Agency to grapple with varied threats and emerging technology.
- (U) T2.0 – **Collaboration** – Following 9/11/2001, T2.0 began to move NSA/CSS from a paradigm of "need to know" to "need to share", both within NSA and with our clients and partners. T2.0 began to merge the Signals Intelligence and Information Assurance missions together as one, providing on-site support and tailored services – which enabled NSA/CSS to fashion new relationships for the new world order, redrawing distinctions between national and tactical, producer and consumer, collector and operator.
- ~~(TS//SI//REL)~~ T3.0 [redacted] Today, NSA/CSS is focused on the [redacted] The intention is to create cooperative, interoperable, real-time Exploitation/Defense/attack-enabling (E/D/enA)[1] capabilities [redacted]

(b)(1)
(b)(3)-P.L. 86-36

[1] (U) NSA/CSS has no CNA or network warfare mission; that mission has been assigned to JFCC-NW. However, many of the capabilities NSA is developing to perform CNE can also be used to enable CNA. For ease of reading, this constellation of capabilities is therefore referred to as "Exploitation/ Defense/attack-enabling or E/D/enA ".

[2] (U) That degree of dominance of one force over another, in the domain of CNO, that permits the conduct of operations by the former and its related comprehensive network capabilities at a given time and place without prohibitive interference by the opposing force.

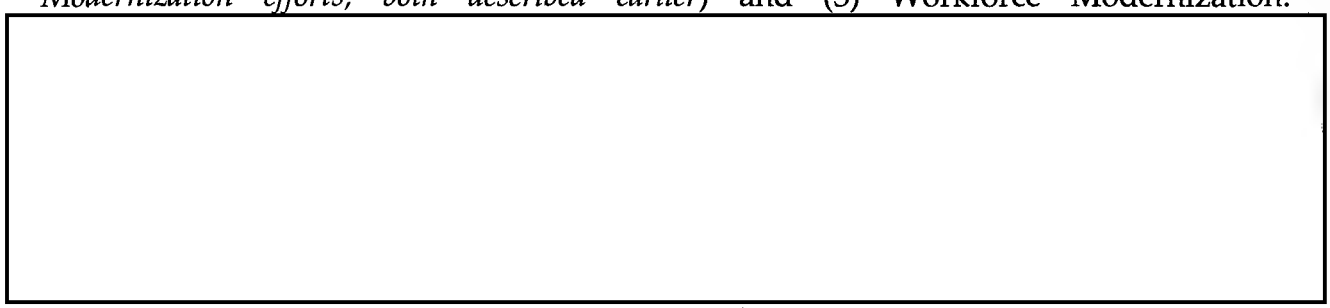


(b)(1)
(b)(3)-P.L. 86-36

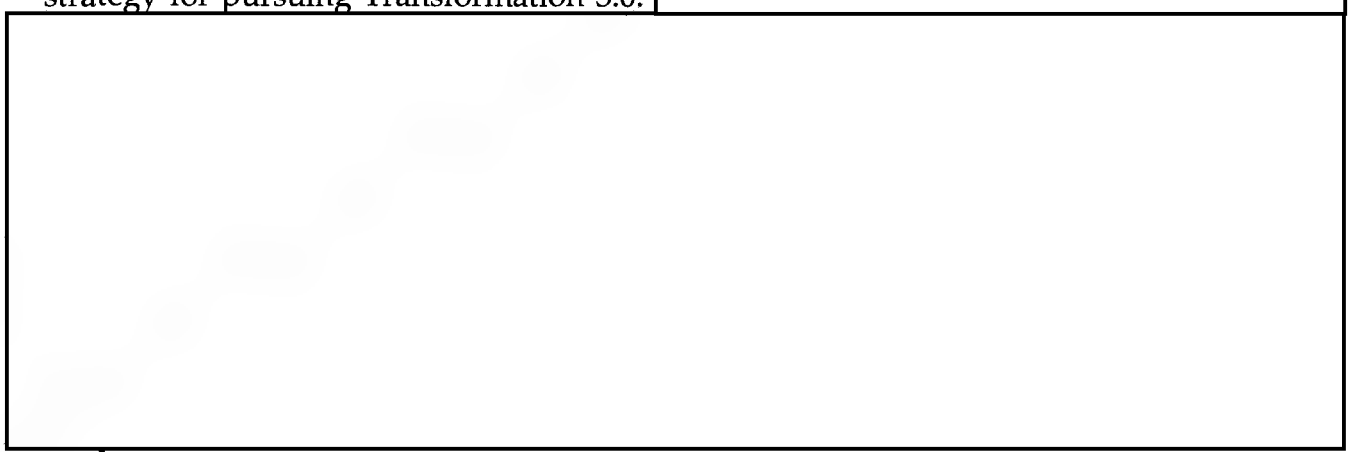
(U) T3.0 is a comprehensive constellation of NSA mission and support activities that will establish a collaborative real-time system of people, processes, and technologies for achieving NSA/CSS' vision of global cryptologic dominance through development and delivery of a National Network Advantage.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL)~~ T3.0, [redacted] is comprised of 3 major initiatives– (1) Mission Modernization, (2) Infrastructure Modernization (*comprising significant improvements in Power, Space and Cooling (PS&C) and Information Technology (IT) Modernization efforts, both described earlier*) and (3) Workforce Modernization.



(U~~//FOUO)~~ Mission Modernization is one leg of a comprehensive three-legged strategy for pursuing Transformation 3.0. [redacted]



[4] (U) The T3.0 Roadmap, the IT Services Initiatives Roadmap, and the Power Space and Cooling (PS&C) Management Roadmap are 36" x 48" plotter printouts, are updated quarterly, and are best viewed at that size.

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

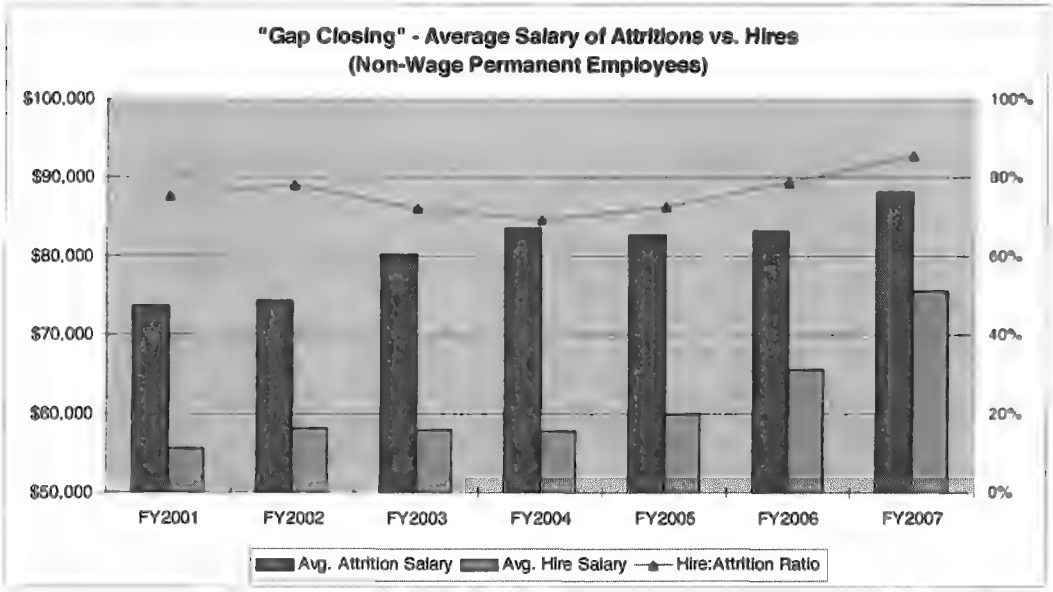
[redacted]

~~(C//REL)~~ Infrastructure Modernization - Modernization of Power, Space and Cooling (PS&C) is one part of a broader NSA effort to address deficiencies in NSA/CSS' mission and support infrastructure, as conveyed by the PS&C Management Roadmap; the other part is Information Technology (IT) Modernization, as conveyed by the IT services initiatives Roadmap. [redacted]

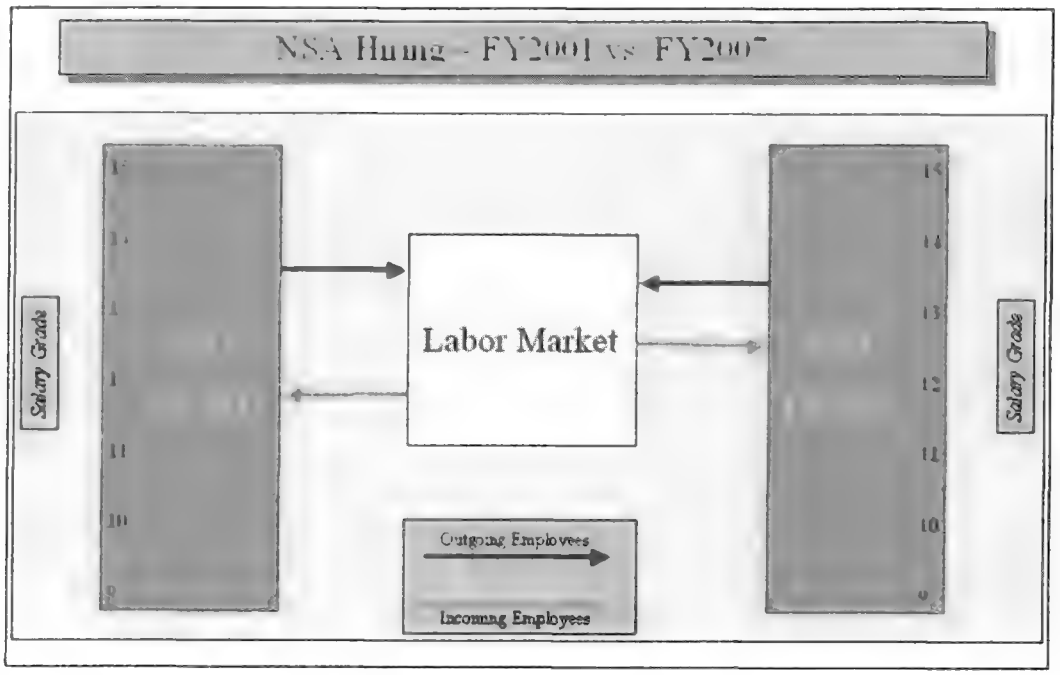
[redacted]

Infrastructure Modernization is an intrinsic enabler to Mission and Workforce Modernization. Therefore, they must all be addressed in a collective and integrated fashion to effectively enable transformation to go forward.

(U~~//FOUO~~) Work Force Modernization – As NSA transforms, changes in the way we operate, collaborate and meet emerging mission requirements demand that we better understand the influence of transformation on the NSA/CSS workforce. This is the central tenet of our Workforce 3.0 Strategy. The revolution in telecommunications, coupled with the changing threat environment, necessitate a transformed workforce that is more mobile, more highly educated, more outward looking, and more experienced. Ultimately, this could mean that workforce costs will increase commensurately with the expanded skills required to meet the threat. NSA/CSS is currently working to better understand what impact T3.0 will have on the pay account and overall workforce dynamics, but early analysis points to the fact that the workforce being created and the collaborative behaviors we are trying to elicit will continue the upward pressure we have seen on pay and competition for the most highly talented people. The graph below shows that the average hiring salary, a key imperative if we're to sustain the workforce to meet emerging threats and challenges, continues an inexorable rise.



Further, besides the pay comparability issues we face in hiring, we are also having to adjust our hiring profiles in terms of grades, to assure we attract the best and brightest in this volatile mid-Atlantic market. The graph below shows the gradual climb in hiring grades, driving outyear adjustments in everything from training to pay considerations to career progression options.



I. (U) FY 2009-FY 2013 Program Build

(U~~//FOUO)~~ In order to build on the successes that NSA/CSS has demonstrated over the last several years, ensure that NSA/CSS continues to provide the actionable SIGINT needed to give warfighters and policy-makers a decisive advantage over our adversaries, and facilitate Transformation 3.0, NSA developed three integrated strategic themes to serve as the framework for the FY 2009 – FY 2013 program. The third theme, specifically vectoring in on the workforce complementing a like theme in T3.0, cites that NSA must maintain a world-class cryptologic workforce and provide them with the tools to assess and defeat the cryptography and complex protocols employed by our adversaries. This will require intensive efforts to compete for, hire, and retain top of the class individuals in mathematics, computer science, and related skills while also providing the specialized processing and computational power needed to address the most intractable cryptologic challenges.

(U~~//FOUO)~~ NSA/CSS has worked to leverage its assets to fully support the *National Intelligence Strategy* since its release in October 2005. Further, NSA/CSS fully supports the DNI's efforts to realize these goals through the 100- and 500-Day Plans, and our program includes funding for a number of initiatives that closely align with the DNI's priorities. We also worked to integrate performance management into our process, as is documented in the performance measures and targets included in our budget submission (to include the requisite human capital related measures). As stated earlier, NSA/CSS has specifically identified human capital and workforce as focus areas in these program years.

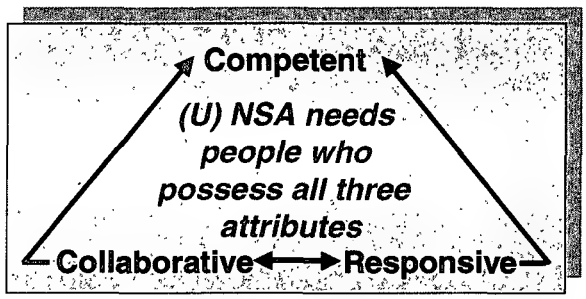
(U~~//FOUO)~~ The workforce modernization focus in this year's budget submission seeks to understand and accommodate the influence that transformation will have on the NSA/CSS workforce by adapting the current workforce to emerging missions and technologies through workforce development and succession planning, by hiring in a targeted fashion to fill critical skill gaps, and by building a workforce that is competent in the areas of expertise required to perform the missions, is able to work collaboratively, and is agile and able to respond quickly when new threats, technologies, and missions emerge.

2. (U) What It All Means

A. (U) Focus Areas

(U) As we assess the present and project the future workforce, many of our skill requirements will stay the same. We still depend on world-class computer scientists, analysts, mathematicians, etc. We still need excellent project managers, contracting

officers, financial professionals and security officers, along with skilled professionals in other support areas.



(U) Due to the dynamic nature of our environment, our workforce must often combine multiple skill sets. The vast majority of the workforce we recruit, reward and retain will demonstrate diverse excellence beyond a single specialty. We need people who are: competent in an area of expertise (e.g., collection, network warfare, cryptography, mathematics or contracting); able to work collaboratively in multiple teams; and, highly responsive when new enemies, technologies and missions emerge.

1. (U) The Nation Expects a High-Level of Competence

(U) There is no substitute for competence. We maintain the required expertise across the breadth of our disciplines, especially in advanced information technologies, and ensure no diminution in our hard-earned reputation for technical excellence across-the-board. This imperative places a premium on mathematicians, computer and information scientists (especially those with a knowledge of global networks), engineers, physical scientists, and analysts who are language proficient and knowledgeable across a wide variety of world cultures.

(U) While deep competency in distinct fields of study/interest is important, so is multidisciplinary expertise. Intelligence analysts, for example, may be called upon to fuse target knowledge, subject matter expertise, familiarity with customers' operational needs/practices, offensive/defensive options, systems engineering, and the tradeoffs between security and operations. This breadth of expertise often takes years to accumulate and NSA/CSS will continue to recognize its extraordinary value through providing necessary developmental opportunities and through supportive Human Capital programs and initiatives.

(U) In addition to cryptologic skills, we need people with proven ability in key areas such as security, acquisition, training, human resources, resources management, logistics, information technology and other enterprise management skills. Such professionals must be knowledgeable of current processes/practices, along with emerging trends, within their respective career fields in order to keep pace with the changing needs of Agency leadership and employee customers and serve as "value added" enablers for the operations professionals.

(U~~//FOUO~~) To help deal with emerging mission sets, new threats and drivers, and to support and facilitate the imperative of change outlined in Transformation 3.0, NSA

developed a comprehensive suite of Focus Areas to help our workforce succeed and contribute in tangible ways.

2. (U) Collaboration Produces the Best Results

(U) We believe that "empowered and enabled" teams produce the most valuable products and services for our customers, partners and stakeholders. This teaming requires our professionals to maintain a range of collaborative skills.

(U) The teams they lead or support may be diverse, matrixed, virtual, multi-disciplinary, multi-service/civilian/contractor. We help our workforce acquire and develop these skills. Our help includes: developing leadership and managerial capacity; invigorating managerial and leadership development; providing professional career road maps; building assessment tools for identifying and assessing the cognitive, emotional and social readiness of individuals to take on leadership roles; and, expanding the use of 360 degree leadership assessments. We also provide the latest tools to enhance collaboration, and then position our people to exploit these tools and other collaborative technologies across the enterprise.

(U) The responsibility to share is also why we are placing more of our analysts in customer and partner spaces (even "virtually"). Embracing the underlying theme to the IC's Civilian Joint Duty program, we understand physical proximity conveys the greatest "feel" by our analysts into the enterprise's changing needs. This emphasis on physical and virtual presence will facilitate the flow of agency knowledge to our customers and partners.

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) The integration [redacted] analysts has allowed collaboration leading to multiple analytic successes over the years. It has also increased our internal diversity in knowledge, experience, expertise and perspective. While there are many social justifications for embracing a diverse workforce, NSA/CSS clearly has a strong mission imperative. To accomplish our ever-changing mission, our people must be able to immediately recognize nuances and complexities across cultures, ethnic groups and social strata. By hiring people with diverse backgrounds (e.g., experience, education, and ethnicity), and ensuring that we develop and retain them, we reduce the risk of "group think" and expand our ability to respond and innovate, advancing our mission performance.

(b)(3)-P.L. 86-36

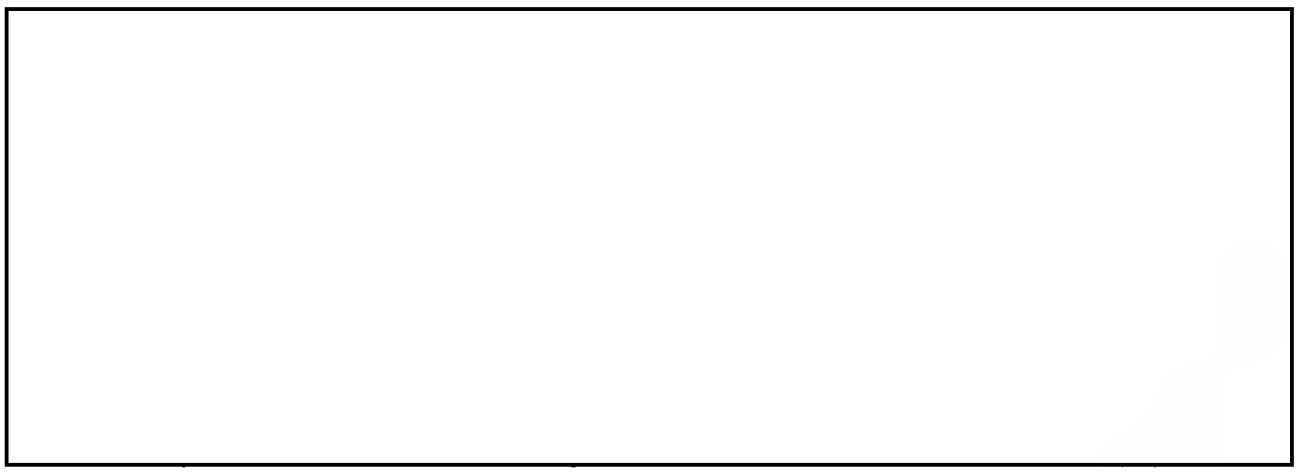
"To combat increasingly complex threats to our nation, the IC must employ, develop, and retain a dynamic, agile workforce that reflects diversity in its broadest context- cultural background, ethnicity, race, gender, and expertise.... We need to have an IC workforce that looks like America and can operate in a global threat environment. We must be relentless in pursuing that goal."
Director McConnell, DNI

(U) Within NSA, we continue to promote greater teaming. We incentivize our workforce to partner across our common network to recognize new threats, devise new solutions and exchange lessons learned. Regular collaboration with co-workers, other directorates, partners and customers is a requirement for today's NSA.

(U) NSA believes in preparing our workforce for success. A host of "enablers" underpin both job assignments and operations. First among these is a forward-looking human resources approach (our workforce strategy mentioned earlier) that obtains and sustains an able and motivated workforce with the right skills at the right geographical locations. Properly sited, provisioned, and secured facilities are also indispensable, as are enterprise IT infrastructure and services that are comparably modern to, but segregated from, less forgiving mission infrastructure and services. Beyond these are other administrative and support specialties such as finance, acquisition, and security.

3. (U) Agile and Responsive to Dynamic Needs

(U) Today's national security environment is as diverse as global society. The multiple threats and customers serviced by NSA/CSS pose requirements that differ in scale, scope and timeliness (compared to those of the past that NSA/CSS was originally formed to combat). As a result, we are realigning our workforce to cover a larger number and wider diversity of enemies/threats, be able to support a greater number of missions, and meet increasing numbers of short-notice/high-priority demands.



We foster a Lean Six Sigma culture that independently, proactively and centrally evaluates and improves our processes and activities in our areas of responsibility.

B. (U) Identifying Requisite Competencies

(b)(1)
(b)(3)-P.L. 86-36

(U~~//FOUO)~~ NSA/CSS acknowledges that the identification and careful management of key attributes needed for the future are vital to transformation in the Human Capital element. To aid this effort, NSA/CSS has identified eight areas and their associated competencies that are described in detail in Workforce Strategy 3.0 "Building the Future Workforce."

Areas	Critical Future Workforce Competencies
Protect (Information Assurance)	
Collection & Operations	
Processing & Exploitation	
Analysis & Production	
Mission Management	
Enterprise IT Investment	
Enterprise Management	
Research	

(b)(1)
(b)(3)-P.L. 86-36

C. (U) Implementation

(U~~//FOUO)~~ To operationalize our strategy and support Transformation 3.0, we developed an implementation plan, laying out discrete goals and objectives focusing on six human capital areas. Further detail can be found in the Implementation Plan itself, but an outline is provided below.

(U) NSA/CSS is focusing our human capital programs on the following capabilities essential to transformation (in order of priority):

1. Converged Networks – Computer Science, Engineering and Mathematics
2. GWOT / Less Commonly Taught Languages
3. Intelligence Analysis
4. Acquisition and Business Management
5. Leadership

(U) To improve on these capabilities, we are further focusing our resources and efforts in the following human capital areas:

Human Capital Areas	Lead GG15 and Below	Lead DISES/DISL	Support
1. Workforce Development	ADET	ADSLM	Mission Elements and Skill Communities
2. Staffing / Succession Planning	ADHR	ADSLM	Mission Elements and Skill Communities
3. Retention and Attrition Management	ADHR	ADSLM	Mission Elements and Skill Communities
4. Workforce Performance Management	ADHR	ADSLM	Mission Elements and Skill Communities
5. Recruiting and Hiring	ADHR	ADSLM	Mission Elements and Skill Communities
6. Occupational Health, Environment, and Safety	OHESS		Mission Elements and Skill Communities

1. (U) Workforce Development

(U~~//FOUO)~~ Workforce development is a key element to the 'productive capacity' of any enterprise. NSA/CSS invests heavily in the education, training and professional development of our cryptologic workforce. The Agency's unique mission as America's' premier Signals Intelligence (SI) and Information Assurance (IA) Agency requires that our workforce stay at the leading edge of knowledge, skills and abilities associated with these disciplines. To meet this mission imperative, we develop and deliver learning activities that tie directly to the desired outcomes of our mission. We invest in on-the-job training, educational opportunities, formal training programs, and other workplace learning activities. As NSA/CSS faces greater scrutiny from Congress, ODNI, and OMB to justify levels of investment, our education, training, and professional development programs must show 'bottom line' contributions to mission success.

(U~~//FOUO)~~ Moreover, the accelerating pace of technology and its use by both the United States and our adversaries demand innovative training and education approaches. Additionally, there is greater emphasis on standardization of business systems and processes at all levels of the federal government. For NSA/CSS, this standardization improves efficiency while enabling better collaboration, both internally, and with other IC and DOD organizations. However, it imposes up-front costs in terms of retraining our workforce to use these standardized business systems and processes.

(U~~//FOUO) In~~ order to deliver the workforce development solutions required for these transformational efforts more effectively and efficiently, and to help the NSA/CSS's enterprise transform, NSA implemented the Enterprise Workforce Development

Capability (EWDC) initiative. The EWDC is a comprehensive solution that encompasses organizational and process changes along with implementing new technologies. Associated with this effort is the plan to have all of the NSA Skill Communities establish career roadmaps that clearly identify workforce competency needs relative to mission requirements.

(U) In addition to the EWDC implementation, NSA/CSS is also focusing on developing a workforce of leaders – both managers and technical leaders. Managers must be capable of dealing with the complexities of diverse, matrixed, virtual, multi-disciplinary, multi-service/civilian/contractor teams in a period of dynamic change. Our people will acquire general business skills, such as communications, project management, strategic and business planning, decision-making, business management, and resource planning and management. We are developing a diverse leadership bench ready to assume positions as managers and technical leaders retire; a process that is running in consonance with ODNI on-going efforts in Leadership Competencies development and the Joint Leadership Development Program.

2. (U) Staffing / Succession Planning

(U) NSA/CSS, like our partners throughout the intelligence community, is facing critical shortfalls of experienced mid-career professionals. We have a disproportionate number of relatively new hires (those hired post-9/11) on one hand, and retirement-eligible professionals on the other. After a decade of tight budgets and constrained hiring in the 1990's, we face a significant challenge in leadership succession and planning.

(U) To maximize our investments in people, we are ensuring we have a robust knowledge transfer process. This process must convey the institutional knowledge of the current workforce to the next generation of Agency employees. The "retirement ready" population of mentors and advisors serves as instructors and on-the-job resources to our less experienced workforce. This is a retention program as well as a knowledge transfer program.

(U) To prepare for the projected number of retirees over the next several years and to ensure smooth transitions, NSA/CSS continues to leverage the Selective Employment of Retirees (SER) and the Standby Active Reserves (SAR) programs. These programs allow us to temporarily hire DOD retirees with specific expertise to fill critical positions and mentor the next generation of Agency employees. Currently, there are over 100 SER/SARs employees across the Agency making up 1% of the NSA workforce. The largest number is in our Signals Intelligence Directorate; they serve as mentors, coaches, advisors and as informal leaders as they work the mission. NSA retirees, prior to leaving the Agency, have the opportunity to express interest in being a member of the Cryptologic Reserve Program (CRP). Interested retirees "register" their availability,

interests, skills and experiences. NSA also coordinates with ODNI and other agencies in the community to ensure compatibility of the CRP with the community-wide reserve program (NIRC), and continues to work across the enterprise to determine if the Reserve Program can satisfy requirements anywhere in the IC.

3. (U) Retention and Attrition Management

(U//~~FOUO~~) Most of our cryptologic workforce has multiple career choices. Twenty percent are eligible to retire before 2010 and the Federal Employees Retirement System covers approximately 80% of our personnel. We know building a cryptologic professional often requires a developmental investment of 3-5 years and at any point that person can leave to apply their talents elsewhere. Therefore, it is absolutely critical that NSA/CSS becomes the competitive "employer of choice" for both tenured (experienced, knowledgeable, and highly productive) professionals and the emerging cohorts of technical and managerial professionals.

(U) To ensure we remain competitive for talent, NSA/CSS is monitoring the compensation market. We understand that compensation is but one factor (albeit a major one) in attracting and retaining top talent. Other factors include desirable job location, opportunity to travel, job security, availability of training, quality of equipment and facilities, and intangibles such as workforce morale, desire for public service, interesting work, etc. In the aggregate, our extraordinarily low attrition rate (about 4% per year, far below private industry norms) leads us to believe we are currently well positioned to compete for talent. However, we also understand that there is no guarantee this position will continue.

(U//~~FOUO~~) Since September 11, 2001, NSA/CSS aggressively implemented a workforce strategy to strengthen transformation through growth, skill alignment, and knowledge transfer. As a result, we significantly increased our population of language and intelligence analysts, computer scientists, engineers and mathematicians. In addition to these new hires, we also understand that the latest generation of recruits brings a different "world-view" about work and careers.

(U) HR monitors and assesses retention and attrition trends and data and develops solutions when an intervention is in order. We continue to use retention bonuses across the enterprise as we transform and build our diverse workforce. We use bonuses to retain critical individuals with vital skills. In some cases we use bonuses to delay the departure of key individuals (allowing for a smoother transition). As more and more Generation X and Y employees enter the workforce with a fluid career model, our refreshment rate may increase. We recognize this possibility, and are prepared to accept shorter careers and manage to greater workforce turnover when appropriate.

4. (U) Workforce Performance Management

(U) NSA is participating in IC efforts to develop and implement a new Human Resources architecture, impacting the work structure, pay structure (pay banding), recruitment and staffing procedures, performance management system, and awards/recognition program. We look forward to managing to these new systems, which we see giving us a market sensitive compensation system providing pay opportunities that enable flexible and effective recruitment, management and retention of a high quality, diverse, high performance workforce with results oriented competencies.

(U//~~FOUO~~) Through our work and compensation structures and the performance management process, we will build a stronger nexus between pay and performance and use our pay budget to our greatest advantage. Defining our work appropriately, maintaining a market-sensitive compensation system, and developing a pay for performance evaluation system will provide the foundation for making compensation and recognition decisions.

5. (U) Recruiting / Hiring

(U//~~FOUO~~) NSA/CSS is shifting the focus of our recruiting and hiring program as we build our diverse workforce of the future. We recruit and hire in a targeted fashion to fill critical gaps that cannot be filled by existing personnel and expand our reach into minority institutions and professional organizations. We use a repeatable model for hiring to ensure alignment with mission and enabling needs on an annual basis.

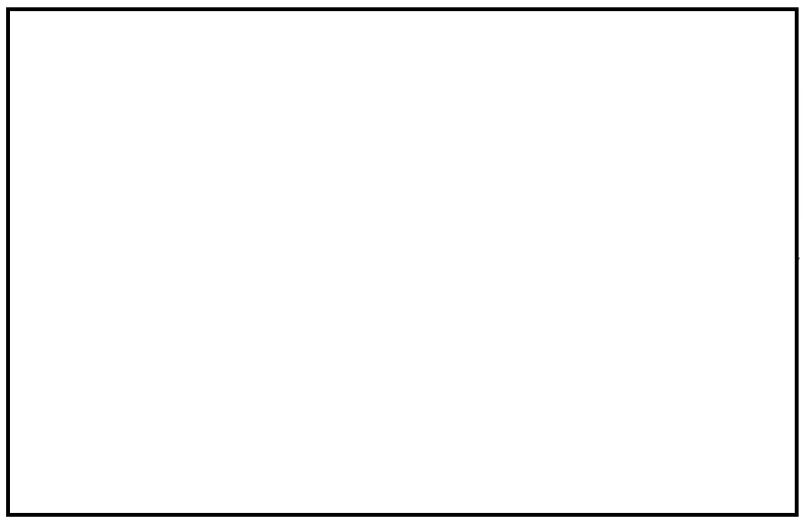
6. (U) Occupational Health, Environment, and Safety

(U) The Agency's mission success is also dependent on the wellness of our workforce, the safety of our workplaces, and the protection of the environment. Occupational Health, Environmental, and Safety Services (OHESS) provides programs to promote and sustain a healthy and safe workplace at NSA/CSS locations worldwide. Besides our ethical and moral obligations to provide these services, they represent a sound business decision, uniquely contributing to mission readiness and assurance. Our programs consistently result in measurable reduction of injuries, illness, mission downtime, absenteeism, and property loss. NSA/CSS' award-winning occupational health, environmental, and safety services continue to play a vital role in overall force protection and ensuring the success of the Agency's mission.

3. (U) Civilian Workforce Profiles

(U~~//FOUO)~~ The NSA/CSS workforce is composed of civilian, military and contractor personnel. This Civilian Employment Plan focuses on civilian resources but there are sizable contractor and military components to the NSA workforce; however, those components are not within the scope of this initial plan. We are planning to address military workforce requirements and issues in the coming weeks as part of an integrated workforce effort. The Deputy Chief, CSS, the Service Cryptologic Elements, the Finance organization and our military HR office made this activity possible through a concerted effort to accurately reflect military personnel in our HR database. In the future, when workforce data compilation methods have more fidelity and accuracy, the agency will develop an overall aggregate workforce employment plan to include contractors and the military components, and which will complement this CEP. In fact, it is envisioned that the future CEPs will become a subset of this overall aggregate agency workforce plan.

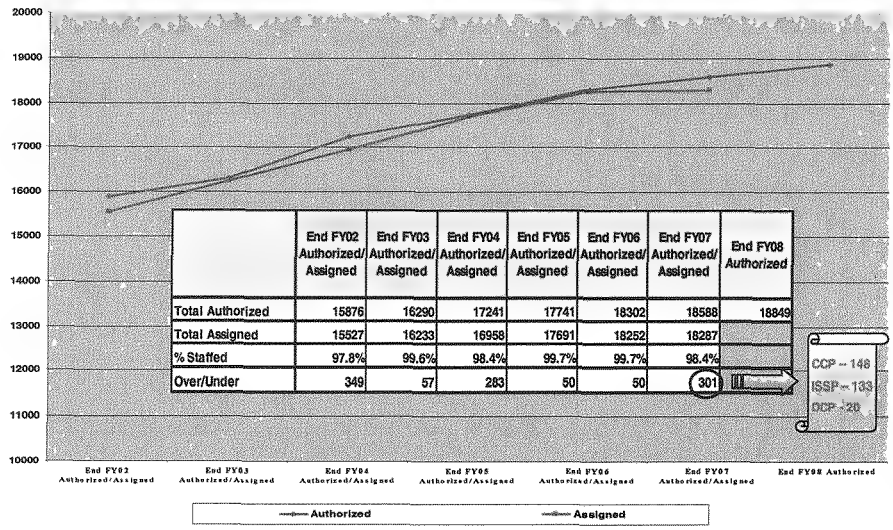
NSA Workforce Composition - Based on FY2007 Authorized End Strength and FY2006 Contractor Inventory



(b)(3)-P.L. 86-36

Our civilian strength has not been static since we stopped downsizing in FY2002. In fact, our authorized strength has grown by 17% since the end of that fiscal year. As shown below, the Agency has been extremely successful in meeting its growth targets and has been staffed at 97.8% -99.7% of authorized strength during this growth period. However, now that NSA is at that level, it creates unprecedented challenges in managing the civilian payroll.

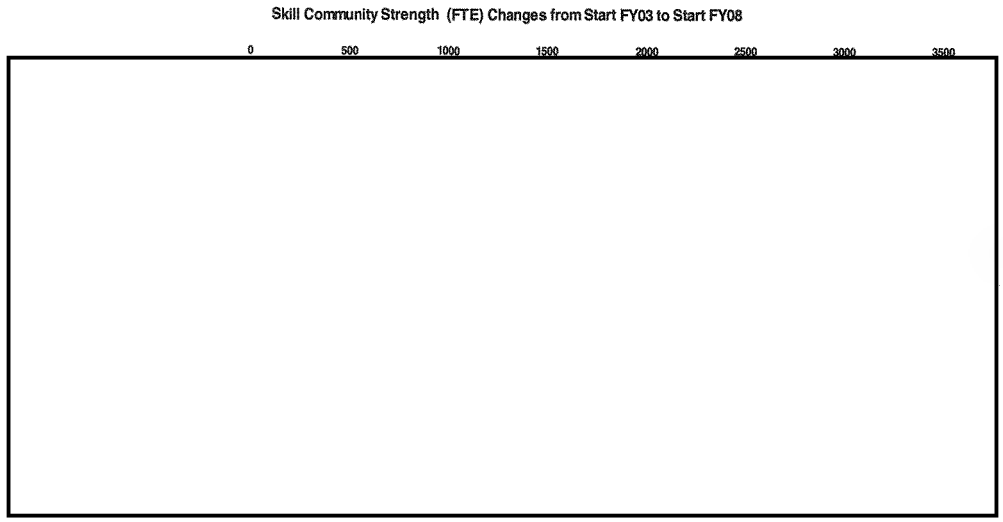
Civilian Authorized/Assigned End FY02 – End FY08
Includes all NSA Civilians (FTE)



	End FY02 Authorized/ Assigned	End FY03 Authorized/ Assigned	End FY04 Authorized/ Assigned	End FY05 Authorized/ Assigned	End FY06 Authorized/ Assigned	End FY07 Authorized/ Assigned	End FY08 Authorized
Total Authorized	15876	16290	17241	17741	18302	18588	18849
Total Assigned	15527	16233	16958	17691	18252	18287	
% Staffed	97.8%	99.6%	98.4%	99.7%	99.7%	98.4%	
Over/Under	349	57	283	50	50	301	

Our strategy has not been growth for growth's sake, but a considered effort to increase our capabilities by employing more technical and analytic personnel and to shore up our security and acquisition functions.

Civilian Population Change Start FY03 – Start FY08
Includes all NSA Civilians (FTE)

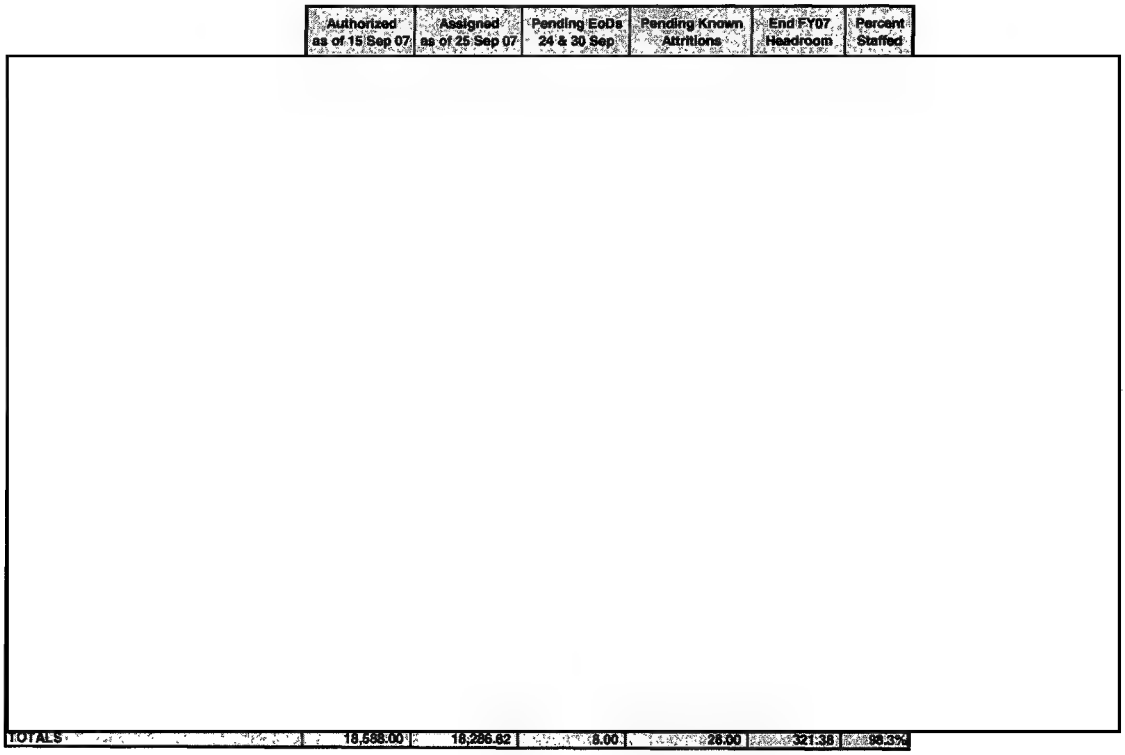


(b)(1)
(b)(3)-P.L. 86-36

(U~~//FOUO)~~ As a result, we have been able to staff all of our major organizations at or very close to their authorized strength levels, achieving balance between mission, enabler and staff functions. Yet, achieving this success has not been easy. In any given

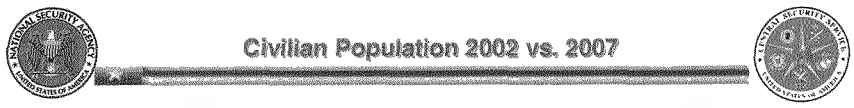
year, we have worked continuously to meet our targets by skill and/or functional area; have exceeded our strength authorization by program or organization due to shortfalls in projected attrition, reassignments or reorganizations; and have been criticized for putting pressure on pay by hiring at mid career, offering incentives for recruitment and retention or awarding high performers.

Current Civilian (FTE) Staffing by Organization Authorized vs. Assigned

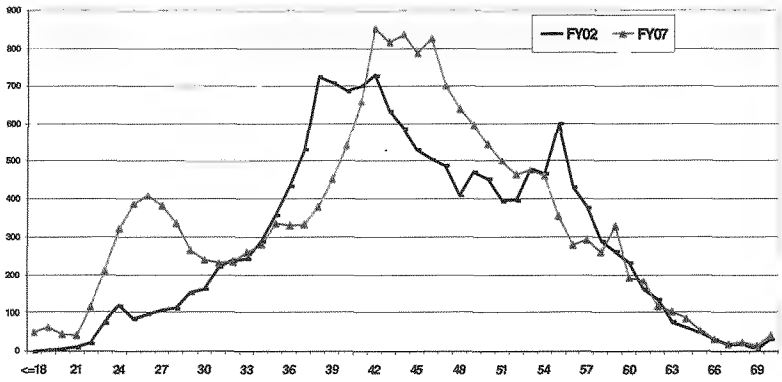


(b)(1)
(b)(3)-P.L. 8

(U~~//FOUO)~~ Additionally, besides the challenges present in "on-boarding" large numbers of new employees, the agency also faces a "graying" of the workforce. Due to large hiring programs in the 1980's, there is a large potential retiree population in approximately 7 to 10 years that must be planned for today. This is especially important since it takes 5 to 7 years to grow a seasoned analyst. Obviously, this means we must hire well in advance of expected seasoned losses, to assure that we have the requisite skills on board at all time. Also, the management challenge is to assure we have the requisite mix of experience to sustain operations during the loss of a significant number of experienced employees. Finally, plans will have to be made to make significant follow-on hiring simply to replace the losses. Ideally, this profile could be smoothed to avoid the cyclical hiring spikes shown below.



Full Time Civilian Population Start FY



(U~~//FOUO~~) As mentioned above, NSA has targeted its accessions to meet emerging and anticipated needs. As the chart below shows [redacted] of the agency's hires were in technical and analytic occupations and another [redacted] were focused on security and procurement-related needs, reflecting Agency as well as IC imperatives.

Hiring Since Start FY 2003 – Start FY2008
(Permanent Civilian FTE Workforce thru 25 Sep 07)

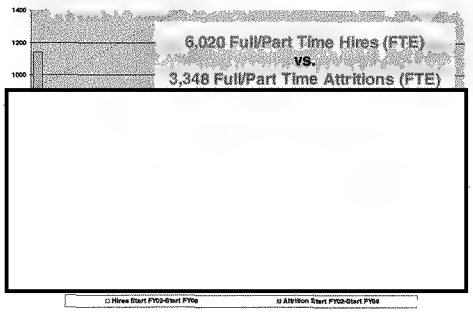
(b)(1)
(b)(3)-P.L. 86-36

6,020 Full/Part Time Hires (FTE)

[redacted] in Technical and Analytic Skills
in Security
in Acquisition & Business (ABM)
in Other

6,020 Full/Part Time Hires (FTE)

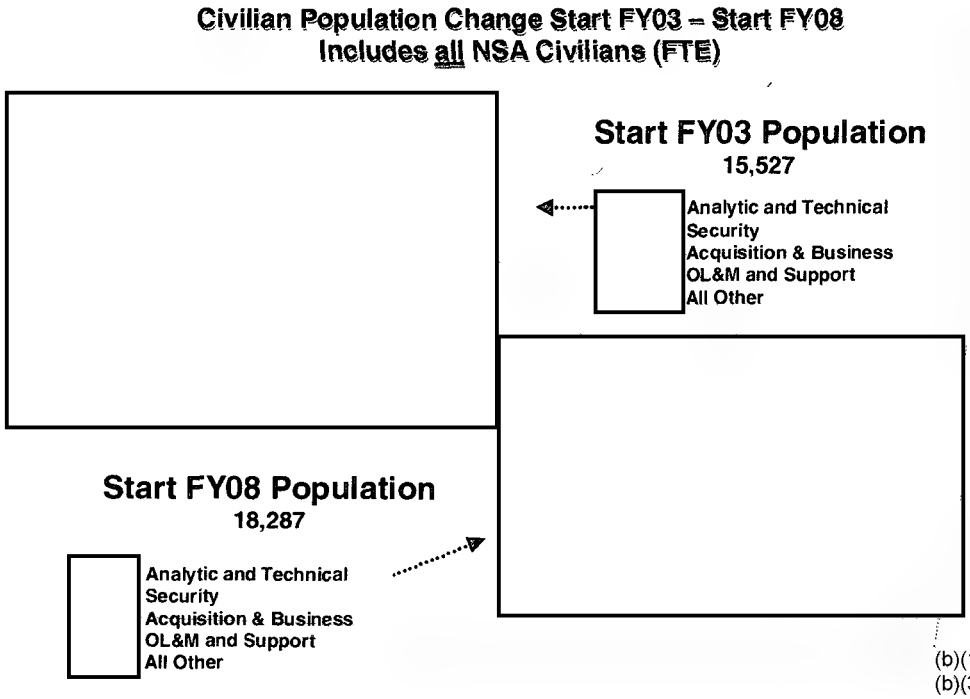
[redacted] Technical
Analytic
Security
ABM
Other
} [redacted] of Hires



(b)(3)-P.L. 86-36

(U~~//FOUO)~~ The Agency has been successful in increasing the number of [redacted]

However, making significant inroads into the overall percentages of the workforce engaged in these activities has proven extremely difficult given the size of the plus ups we have been granted. Since a percentage of our hiring program every year must be allocated to replace attrition to support on-going operations, it is difficult to make major shifts in the overall makeup of the workforce.



(b)(1)
(b)(3)-P.L. 86-36

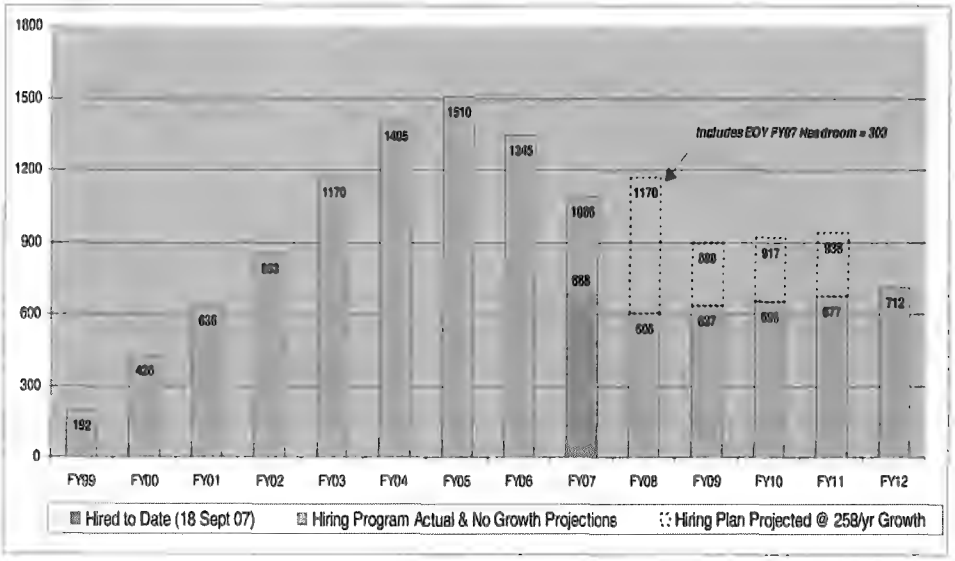
~~(C//REL)~~ The Agency's hiring programs are projected to be approximately 800 to 1300 per year depending on future plus ups (currently planned at 250 per year through FY11), attrition and the number of vacant positions left at the close of any particular fiscal year.

In watching our profiles, there are some trends that serve as examples of the dynamics that we consider:

[redacted]

Our outyear budget program is targeted to allow us to continue to invest in critical technical and analytic skills, but it is limited to essentially maintaining current staffing levels in key enabler organizations due to the scope. Consequently, our T3.0 initiatives seek to internally adjust existing resources to best mitigate emerging needs. As these efforts take more shape, we'll be able to report on them in subsequent CEPs.

FY99 through FY12 FTE Hiring Programs



(U) Conclusion

(U) NSA/CSS's dedicated, integrated Human Capital Strategic Planning process establishes the foundational support and key activities for workforce management at NSA/CSS from FY08 – FY10, and beyond. This is a dynamic process and will continually be improved as the Agency continues its transformation efforts. Further, this process is consciously and deliberately embedded as a major tenet of the Agency's overall transformation efforts, and is a full partner with complementary efforts in facilities planning, IT strategic visioning, resources apportionment, and budget and program planning. The complex and rapidly changing global environment continues to increase the pressure on us to adjust our workforce to handle any situation, anywhere, at anytime, recognizing that we are dealing with finite and extremely valuable resources. Our goal is to meet today's challenges while strategically planning for the future and making the best investment in our greatest asset – the people of the NSA/CSS.

The NSA/CSS Budget Picture—Magnitude and Focus

Funding Sources and Purposes

(U//~~FOUO~~) NSA/CSS is funded through three programs: the Consolidated Cryptologic Program (CCP), an element of the National Intelligence Program (NIP) administered by the Director of National Intelligence; the Military Intelligence Program (MIP), administered by the Under Secretary of Defense for Intelligence; and the Information Systems Security Program (ISSP), administered by the Assistant Secretary of Defense for Network Integration and Information.

~~(S)~~ Our Signals Intelligence (SIGINT) mission is funded by the CCP and the MIP. The NSA/CSS SIGINT mission supports all U.S. foreign intelligence customers, both military and non-military. However, we also have certain projects specifically directed to support military customers. Funding for our SIGINT work is broken down along these lines.

- With CCP funds [redacted] we carry out the *national-level* U.S. Signals Intelligence (SIGINT) mission, i.e., those aspects of NSA/CSS SIGINT mission that benefit *all SIGINT customers* [redacted] (b)(3)-P.L. 86-36

  [redacted]

- With MIP funds, NSC/CSS conducts SIGINT-related activities that are *specifically designed to benefit Defense Department and military customers.*

  [redacted]

(U//~~FOUO~~) The NSA/CSS Information Assurance (IA) mission is funded in the ISSP. In the IA mission, NSA/CSS helps keep critical national security information, systems and networks safe against theft, tampering and destruction. We provide solutions, products, and services, and fund defensive information operations, to achieve information assurance for information infrastructures critical to US national security interests.

Funding Levels

(b)(1)
(b)(3)-P.L. 86-36

Current and Long-Term Funding Levels

[redacted]

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

[redacted] These funds are allocated among the three programs as follows:

	FY-09 Appropriated	FY-10	FY-10/15
CCP	[redacted]		
MIP			
ISSP			
TOTAL			

(b)(3)-P.L. 86-36

Appropriations Types

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

The percentages remain relatively constant from year to year.

Manpower and Payroll

~~(S//NF)~~ NSA/CSS has approximately 37,000 positions in total. Of these, [redacted] positions are funded within the CCP [redacted] The ISSP has approximately [redacted] The MIP has [redacted]

~~(S//NF)~~ Within the base program numbers shown above, the NSA payroll cost is [redacted] These figures cover only *civilian* payroll; pay for military personnel is funded by the respective military services and is not included in the payroll cost shown here.

Supplemental Funding

~~(S)~~ The previous discussion does not take into account supplemental funding, which is approved by Congress on a year-by-year basis and not reflected in our long-term budget profile. Over the past several years, NSA/CSS has received supplemental funding [redacted] Supplemental funding allows NSA/CSS to provide intelligence that we expect our customers will require for the foreseeable future.

~~(S)~~ To continue our current level of performance, we expect to require approximately [redacted] above and beyond the amounts

[redacted]

currently reflected in the base program. This figure is consistent with the Administration's supplemental requests for FY-09 and FY-10 as follows:

	FY-09	FY-10
CCP		
MIP		
TOTAL		

[redacted] appropriated to date [redacted] not yet appropriated

(b)(1)
(b)(3)-P.L. 86-36

Investment Areas

CCP – Overview

~~(S//SI)~~ The CCP funding that NSA/CSS receives is allocated among a variety of budget categories, known as Investment Portfolios. These categories are the same for all organizations that receive funds from the National Intelligence Program. Following are two breakdowns of CCP funding by Investment Portfolio. Figure 1 shows total base program funding (payroll and non-pay) for FY-09 and FY-10 while Figure 2 shows a similar breakout excluding payroll costs.

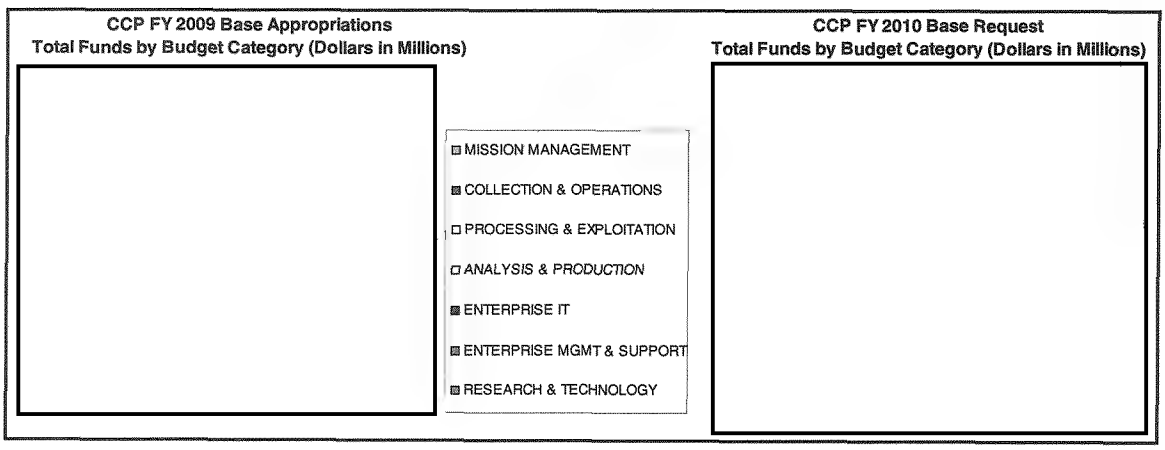

CCP FY 2009 Base Appropriations
Total Funds by Budget Category (Dollars in Millions)
CCP FY 2010 Base Request
Total Funds by Budget Category (Dollars in Millions)
MISSION MANAGEMENT
COLLECTION & OPERATIONS
PROCESSING & EXPLOITATION
ANALYSIS & PRODUCTION
ENTERPRISE IT
ENTERPRISE MGMT & SUPPORT
RESEARCH & TECHNOLOGY

Figure 1

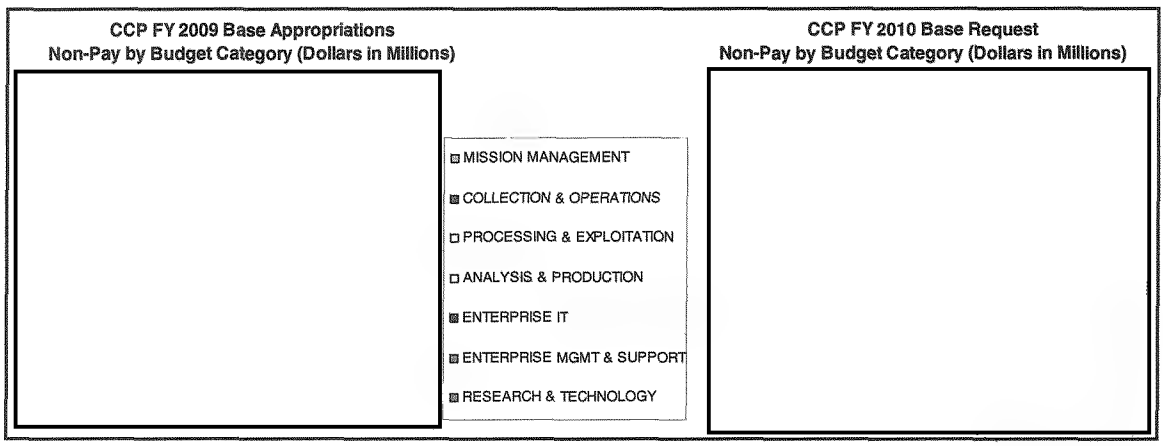

CCP FY 2009 Base Appropriations
Non-Pay by Budget Category (Dollars in Millions)
CCP FY 2010 Base Request
Non-Pay by Budget Category (Dollars in Millions)
MISSION MANAGEMENT
COLLECTION & OPERATIONS
PROCESSING & EXPLOITATION
ANALYSIS & PRODUCTION
ENTERPRISE IT
ENTERPRISE MGMT & SUPPORT
RESEARCH & TECHNOLOGY

Figure 2

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI)~~ Across those Investment Portfolios, the CCP budget addresses four interdependent focus areas: 1) sustaining current operational activities in the face of a dramatically increased, and constantly evolving, operations tempo; 2) modernizing the aging information technology (IT) and physical plant infrastructures to ensure robust support to critical mission activities; 3) transforming the cryptologic enterprise to keep pace with relentless and rapid changes in target behaviors and technological advances; and 4) supporting efforts to secure cyberspace via providing information on, and responding to, cyber threats to the United States as part of the Comprehensive National Cybersecurity Initiative (CNCI).

Ongoing Operations

~~(TS//SI//NF)~~ Regarding the current operations tempo, NSA/CSS is pursuing three principal mission imperatives: ensure effective and actionable SIGINT for a myriad and diverse customer set in support of national interests and operational campaigns; exploit hard targets; and provide the global intelligence [redacted] analytic tradecraft, and operational infrastructure needed to provide information on, and to respond to threats to the United States. The pace of current operations is daunting and we must ensure that we continue to sustain our operational capabilities to meet customer requirements for critically needed SIGINT and information assurance.

Infrastructure Modernization

(U~~//FOUO)~~ We must also ensure that we have a robust IT infrastructure and that our facilities – for people and equipment – are adequate to today's mission requirements. The IT effort includes modernizing campus area and wide area networks, servers, desktops, directory services, software licensing, and information assurance for NSA/CSS systems.

(U~~//FOUO)~~ Facilities modernization includes both constructing new, state-of-the-art facilities that will enhance mission accomplishment, and rehabilitating and improving existing facilities. A major focus of this work is to create sufficient power, space and cooling capacity to meet the demands of today's information storage and processing

equipment. The power, space, and cooling effort addresses both power capacity and reliability as well as the sustainment of existing facilities and the reduction of the backlog of maintenance and repair.

Mission Transformation

~~(TS//SI)~~ Three integrated strategic themes serve as the framework for NSA/CSS transformation activities:

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

First, we must possess the *global reach* necessary to gain access to diverse communications and to develop and deploy [redacted]

Second, we require *world-class diagnostic capabilities* that will enable us to find adversaries [redacted]

Third, we must maintain a *world-class cryptologic workforce* with the tools to assess and defeat cryptography and complex communications protocols employed by our adversaries. This requires the hiring and retention of top-of-the-class individuals in mathematics, computer science, and related skills as well as specialized processing and computational power to address the most intractable cryptologic challenges. Additionally, we must continue efforts to hire and retain the language analysis and business management expertise required to prosecute the NSA/CSS mission.

Cyber Security

~~(S//NF)~~ It has become increasing clear how our Nation's critical information systems and infrastructure – including those critical to our national defense and other core governmental functions – are to intrusion, theft, and damage through cyber-attacks. To address this threat, the Administration developed the Comprehensive National Cybersecurity Initiative (CNCI), for which Congress began allocating funds during Fiscal Year 2009.

(b)(3)-P.L. 86-36

~~(S//NF)~~ [redacted]

	FY-09 Appropriated	FY-10	FY-10/15
CCP			
ISSP			
MIP			
TOTAL			

(b)(1)
(b)(3)-P.L. 86-36

~~(S//NF)~~ The objective of the CNCI is to achieve a greatly enhanced understanding of cyber threats and vulnerabilities in order to reflect real-time situational awareness of the cyber environment and to provide robust active cyber defense. It seeks to establish a front-line of cyber defense, attribute the source of malicious activity, block or limit the effectiveness of such activity, understand the capabilities and intensions of those who launch such activities, and provide the United States with well-informed options for an integrated operational response. In short, the CNCI demonstrates the resolve to secure US cyberspace and set the conditions necessary for long-term success and to shape the future cyber environment to secure the US technological advantage.

MIP Overview

~~(S//NF)~~ Our troops in harm's way have unique and urgent intelligence needs.

(b)(1)
(b)(3)-P.L. 86-36

The NSA/CSS MIP is focused on making sure this occurs.

~~(S//NF)~~ NSA/CSS programs funded by the MIP

The elements of the armed services that team with us to carry out the cryptologic mission are called the Service Cryptologic Elements (SCEs). Within the MIP, our goal is to make the SCEs fully capable mobile component of a single, global, integrated, cryptologic system.

~~(S//NF)~~ To accomplish this, there are three main foundational thrusts that cut across the NSA/CSS MIP budget:

(b)(1)
(b)(3)-P.L. 86-36

Following are two breakdowns of MIP funding by mission capability. Figure 3 shows total base program funding (payroll and non-pay) for FY-09 and FY-10 while Figure 4 shows a similar breakout excluding payroll costs.

(b)(1)
(b)(3)-P.L. 86-36

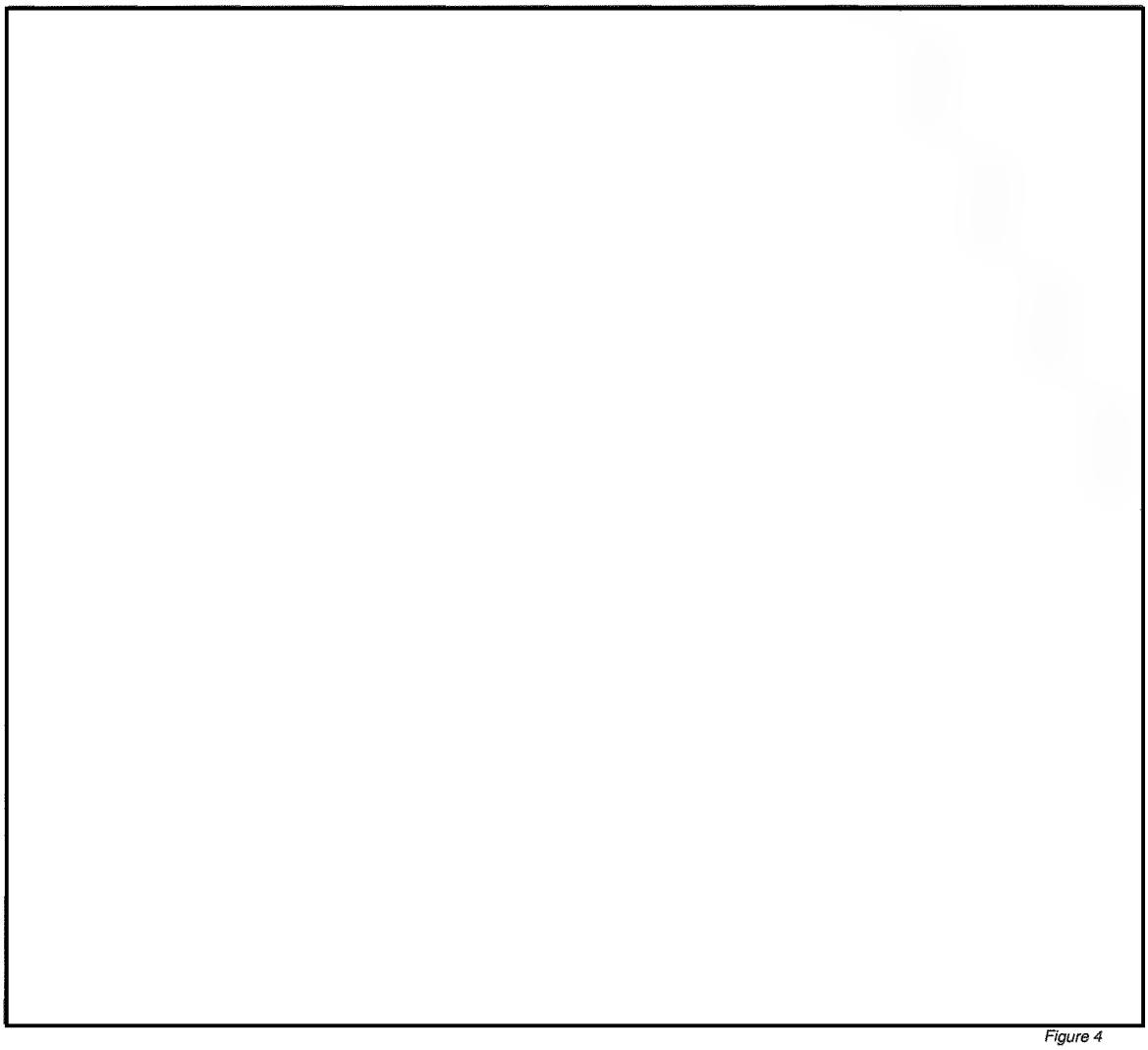


Figure 4

ISSP Overview

(U~~//FOUO)~~ The ISSP is focused on providing the information assurance solutions, services, infrastructure, and capabilities necessary to enable clients to assure the safe continuity of business and mission operations through the use of automated information systems and information sharing while precluding unauthorized actions that can lead to disclosure of sensitive information, modification or destruction of data, theft of data; impersonation or misrepresentation of authorized system users by unauthorized users, and denial of service.

(U~~//FOUO)~~ The ISSP budget supports traditional information assurance core capabilities, such as information assurance guidance and security engineering; provides increased vulnerability analysis and operations to mitigate the threat to, and vulnerabilities of, information systems and to increase knowledge of the adversary; [redacted] focuses on enterprise security management; seeks a balanced mix of GOTs and COTs products; [redacted] and

(b)(3)-P.L. 86-36

focuses on investments in those activities for which NSA can provide unique information assurance value.

~~(S//NF)~~ Following are two breakdowns of ISSP funding into its major components aligned to DoD information assurance goals. Figure 5 shows total base program funding (payroll and non-pay) for FY-09 and FY-10 while Figure 6 shows a similar breakout excluding payroll costs.

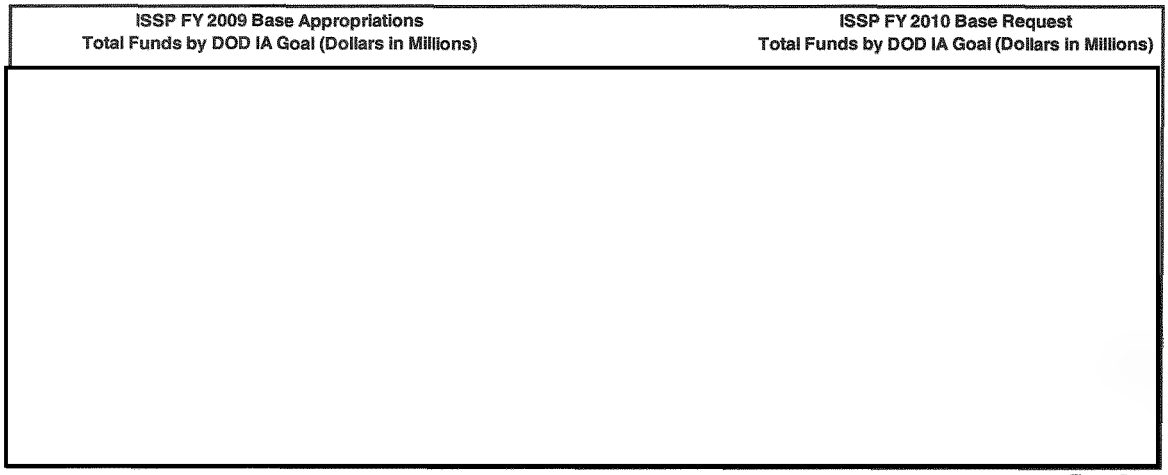

ISSP FY 2009 Base Appropriations
Total Funds by DOD IA Goal (Dollars in Millions)
ISSP FY 2010 Base Request
Total Funds by DOD IA Goal (Dollars in Millions)

Figure 5

(b)(1)
(b)(3)-P.L. 86-36

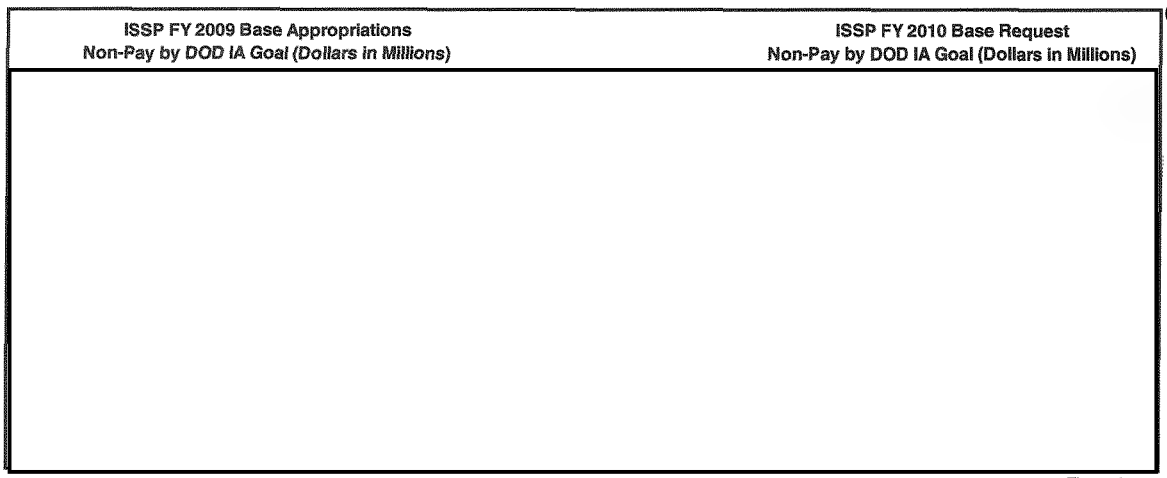

ISSP FY 2009 Base Appropriations
Non-Pay by DOD IA Goal (Dollars in Millions)
ISSP FY 2010 Base Request
Non-Pay by DOD IA Goal (Dollars in Millions)

Figure 6

~~(S//NF)~~ The ISSP budget provides the resources to:

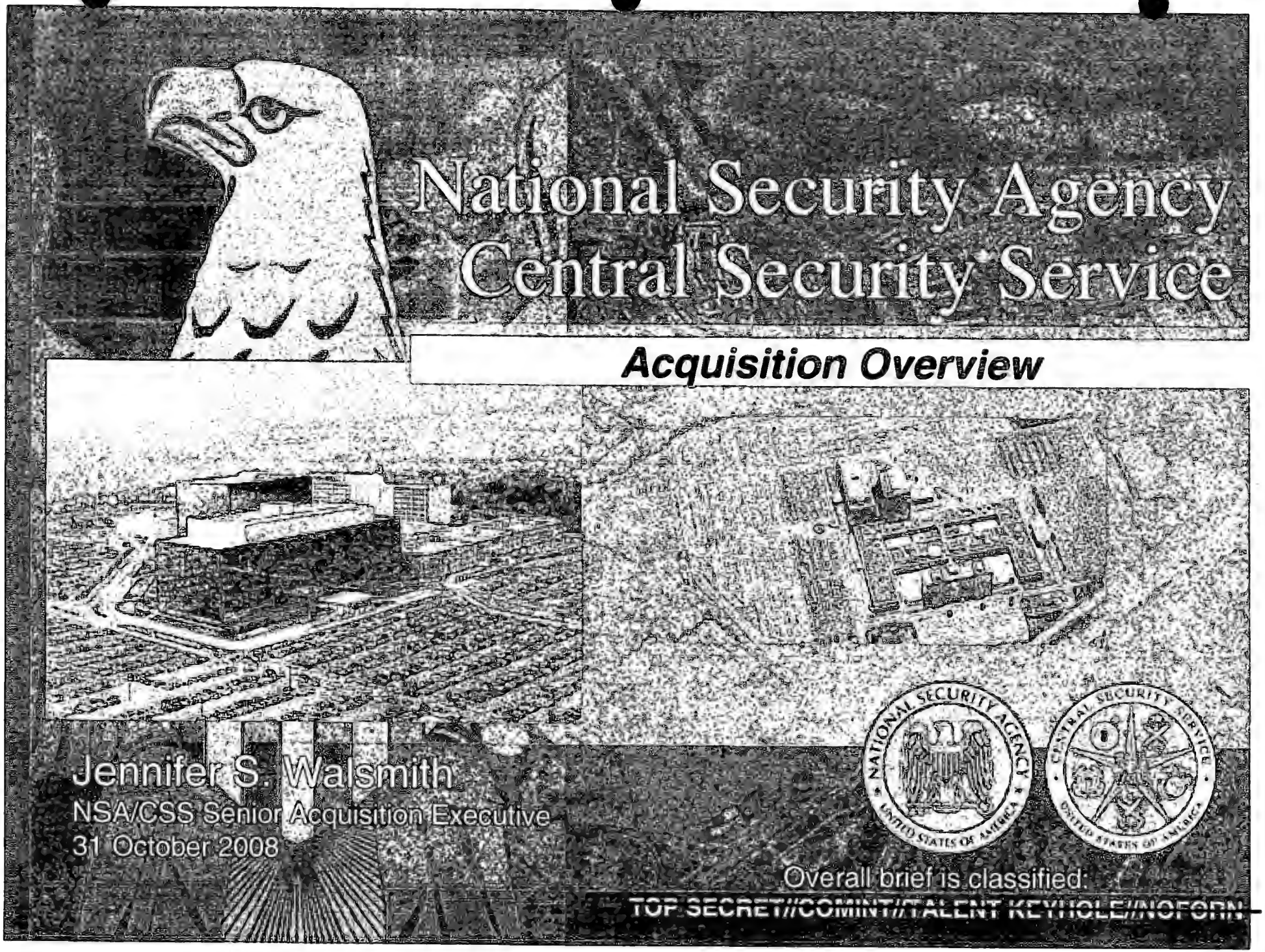
- protect information by safeguarding data as it is being created, used, modified, stored, moved, and destroyed to ensure that all information has an appropriate level of rust;
- defend systems and networks by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and systems and networks are capable of self-defense;

- provide information assurance situational awareness [redacted]
- transform and enable information assurance capabilities by [redacted] (b)(1) (b)(3)-P.L. 86-36
- create an empowered workforce that is well equipped to support the information assurance mission.

(b)(3)-P.L. 86-36

CONCLUSION:

(U~~//FOUO)~~ NSA/CSS is a valued, and increasingly valuable, commodity for the Defense and Intelligence communities. Only NSA/CSS has the combination of global presence, operational perspective, technology expertise, and analytical skills to achieve network superiority for the United States. The NSA/CSS budget seeks to ensure that NSA/CSS remains a vital national asset by funding initiatives that are critical to, and provide a significant return on investment for, the future security of the nation.


National Security Agency
Central Security Service
Acquisition Overview
Jennifer S. Walsmith
NSA/CSS Senior Acquisition Executive
31 October 2008
Overall brief is classified:
TOP SECRET//COMINT//TALENT KEYHOLE//NOFORN

Agenda

- Acquisition Vision & Mission
- Acquisition Strategic Objectives
- Acquisition Support to NSA
- Organization/Layout
- What NSA buys
- 2008 Procurement Overview
- 2008 Small Business Performance
- Tier 1 Program Summary

Acquisition Vision & Mission

Vision

Be a world-class acquisition organization for NSA to enable and sustain superiority by:

- Empowering a knowledgeable, skilled, and effective workforce
- Providing acquisition leadership, oversight, and support
- Creatively implementing best practices
- Applying effective life-cycle management

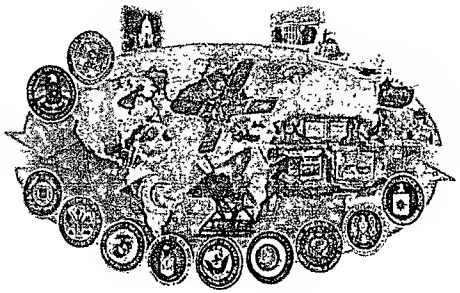
Mission

The mission of the Acquisition Organization is to acquire and sustain capabilities, systems, products, and services through a disciplined, yet agile, process that enables NSA to continually modernize efficiently and effectively.

Acquisition Strategic Objectives

- Develop, deliver, and field capabilities rapidly that meet our operational mission needs within cost, schedule, and performance through diligent execution and well laid out program plans
  - Streamline and tailor acquisition process from requirements through delivery
  - Provide expert program management and agile acquisition oversight
- Assure an agile, diverse, trained, certified, skilled, valued, motivated and Cryptologic savvy workforce
- Inject new ideas and technologies into the transformation architecture and to enable information superiority by finding new ways to tap an expanded industrial base
- Continually assess return on investment for all acquisition activities
- Provide timely response to all customers in procuring needed materials, contracting goods and services, and managing acquisition activities that support the Cryptologic mission
- Build overseer, stakeholder, and customer confidence in NSA's investment programs, program management abilities, and oversight

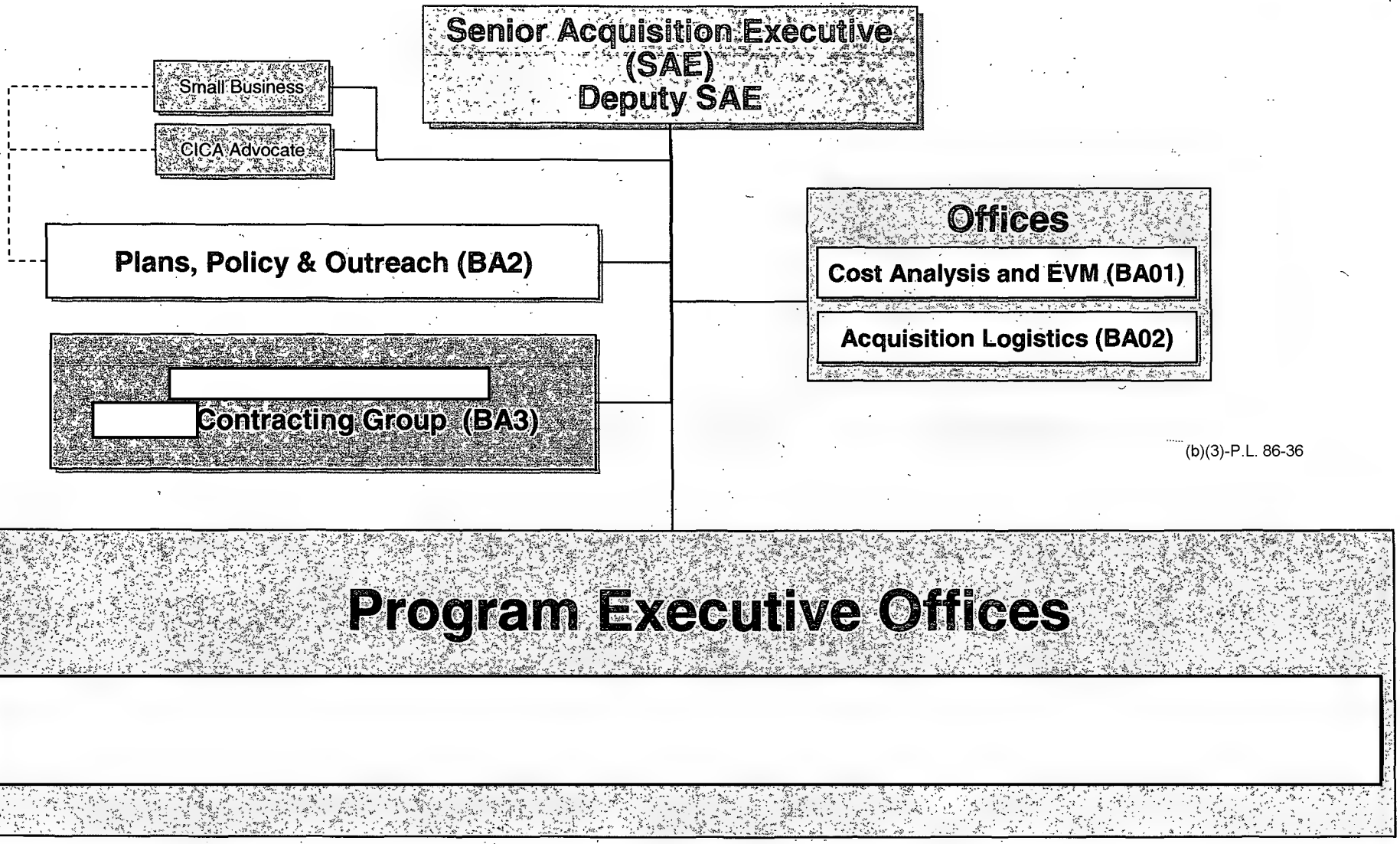
Acquisition/PEO Layout



Support National/Military Objectives

(b)(1)
(b)(3)-P.L. 86-36

Acquisition Organization



What NSA Buys...

- IT Services
- Hardware
- Middleware
- Software
- [redacted]
- Facilities Engineering
- System Engineering
- Program Management
- Business Systems
- [redacted]
- Snow Removal
- Power from BG&E
- Building (lease from Army Corps)
- Landscaping Services
- Electrical Services
- [redacted]
- Testing Services
- Software Systems
- Tools

(b)(3)-P.L. 86-36

2008 Procurement Overview

- 60% Competition
  - Sole source for small business set-asides, niche technologies, unique capabilities, and urgent mission needs
- [redacted] awards (with only [redacted] unlimited contracting officers)
- 25% of Budget went to Small Business Prime Contracts (b)(3)-P.L. 86-36
- Over [redacted] companies registered in the NSA Acquisition Resource Center's database (main repository for market surveys)

~~(U//FOUO)~~ Obligation Rates:

[redacted]

~~(U//FOUO)~~ Outlay Rates:

[redacted]

(b)(3)-P.L. 86-36

~~(S//SI)~~ **FY08 Total Actions Awarded** [redacted] **awards)**

[redacted]

Dollars obligated last 4 years by Contracting (b)(1) (b)(3)-P.L. 86-36

2008 Small Business Performance

Prime Contracting Category	FY08 NSA Goal (%)	FY08 Actual (%)
Small Business Overall	26%	25.2%
Small Disadvantaged	5%	6%
Women Owned	3%	3%
HUB Zone	.75%	.5%
Service Disabled Veteran	1%	1%

- ***Did not meet overall small business goals, however, increased SDVOSB by 500% and surpassed DoD goal of 22.4%***
- ***Cited as a Small Business Center of Excellence for the 1st Half of FY2008***

NSA/CSS Tier 1 Program Summaries

Financial Accounting and Corporate Tracking System (FACTS)

Program Description: (U~~//FOUO)~~ FACTS provides NSA/CSS with modern, secure, leading edge business solutions that will comply with external regulatory guidance and audit requirements, achieve standardization and integration of business systems and processes, and deliver credible business information needed for mission success.

Increment 1: (U~~//FOUO)~~ The following functionality was delivered and went operational on the following dates:

FACTS Release 1.0 (Budget Loading and Financial Planning Management) – Mar, 07

Release 1.1 (Procurement Requests for Initiation and Spend Plans) – May, 07

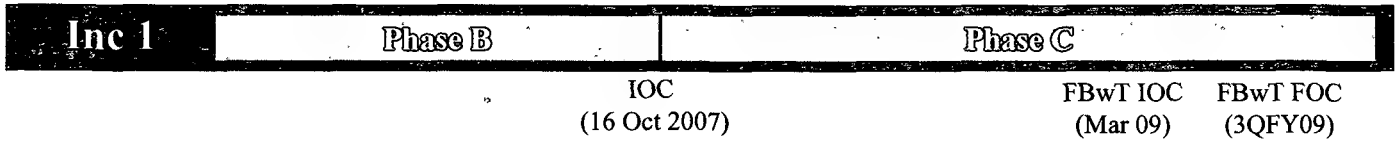
Release 1.2 (General Ledger, Purchasing, and Reimbursable Agreements) – Oct 07

Increment 2: (U~~//FOUO)~~ The following activities and capabilities are planned:

Funds Balance with Treasury (FBwT) - Initial Capability (Mar 09); Complete Capability (3QFY09)

Complete Migration of [redacted] financials onto FACTS (4QFY10) (b)(3)-P.L. 86-36

Program Schedule:



Program Manager: [redacted]

Prime Contractor(s): Accenture National Security Services, LLC

(b)(3)-P.L. 86-36

Program Funding

Current Year (FY09): [redacted]

Future Years (FY10-15): [redacted]

*This funding includes both FACTS and BITMAP resources.

Business IT Modernization Auditability Program (BITMAP)

Program Description: (U//~~FOUO~~) The BITMAP program is a transformational initiative for the NSA/CSS to develop and meet the audit requirement as specified by ODNI and directed by the CFO Act. In addition, this initiative supports the NSA/CSS Transformation 3.0 goal

(b)(3)-P.L. 86-36

Increment 1: (U//~~FOUO~~) BITMAP Increment 1 will deliver key functionality in four key areas required for auditability: Asset Management (AM), Supply Chain Management (SCM), Project Costing (PC), and Time and Labor (T&L). These capabilities must incorporate new and existing business systems and processes to ensure auditability for NSA/CSS

Program Schedule:

Inc 1	Phase A	Phase B	Phase C
		MS B (4QFY09)	IOC/MS C (4QFY10)

Program Manager:

Prime Contractor(s): Accenture National Security Services, LLC
Deloitte Consulting

(b)(3)-P.L. 86-36

Program Funding
Current Year (FY09):
Future Years (FY10-15):
*This funding is includes both FACTS and BITMAP resources.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

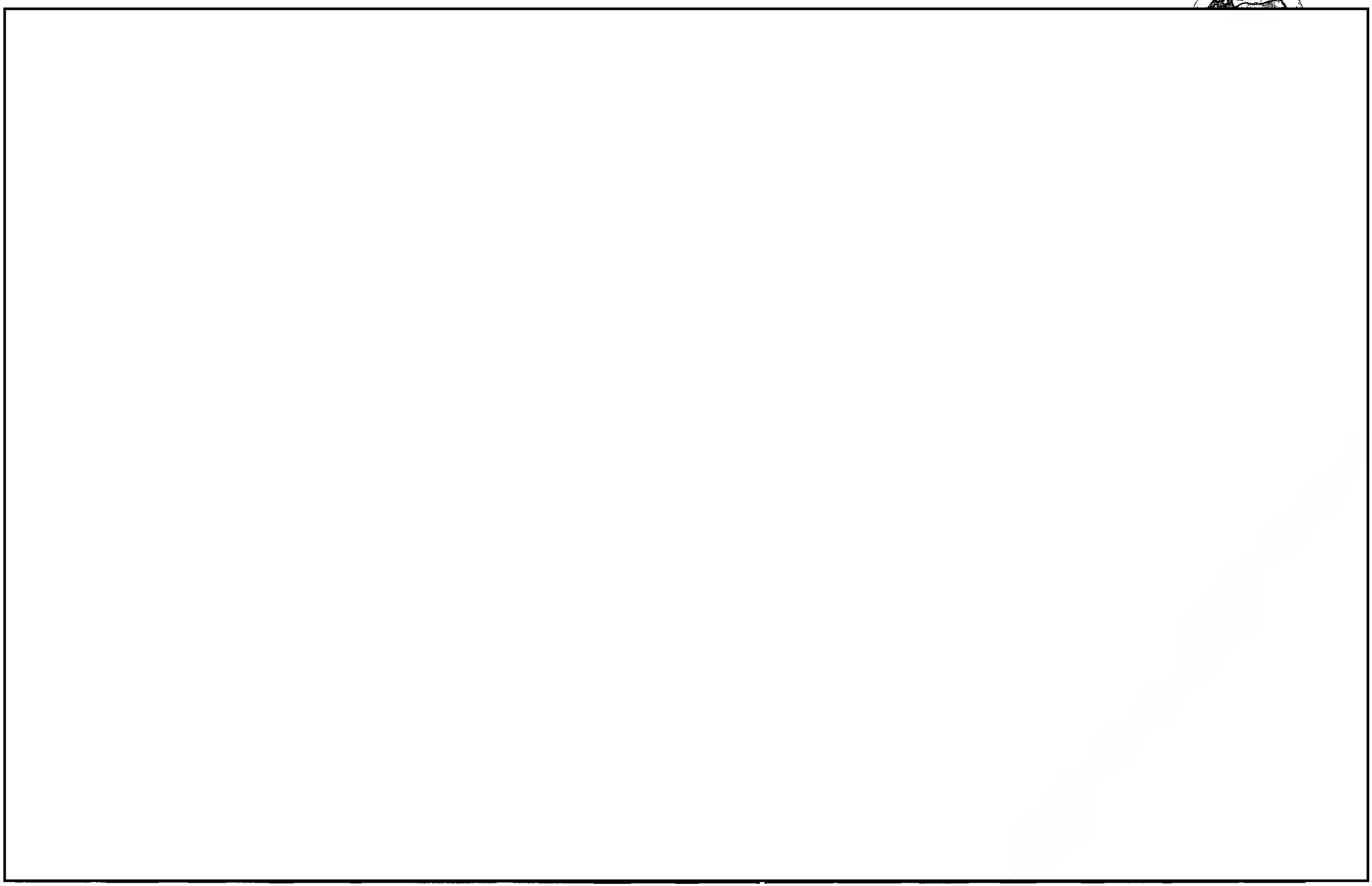
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

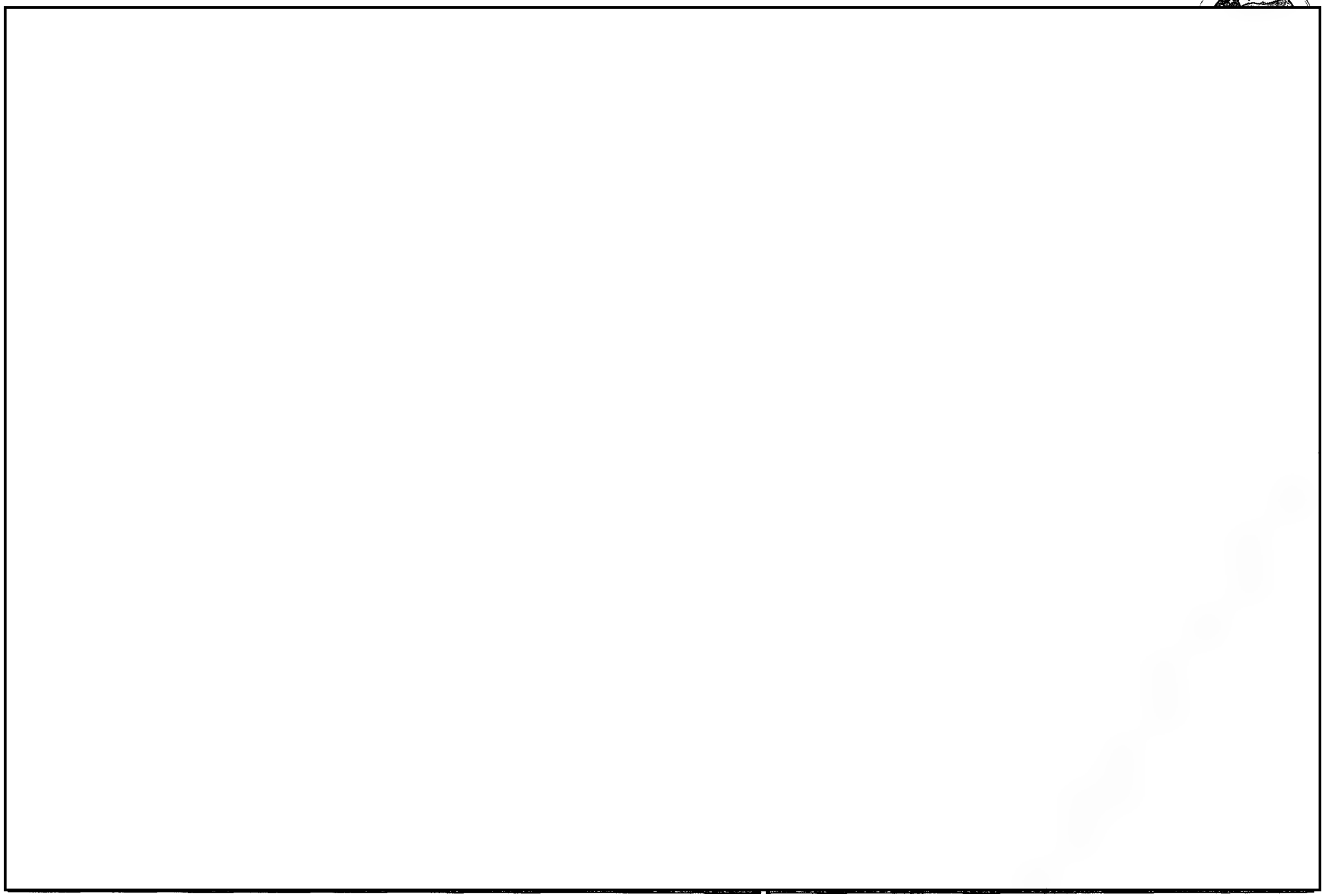
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

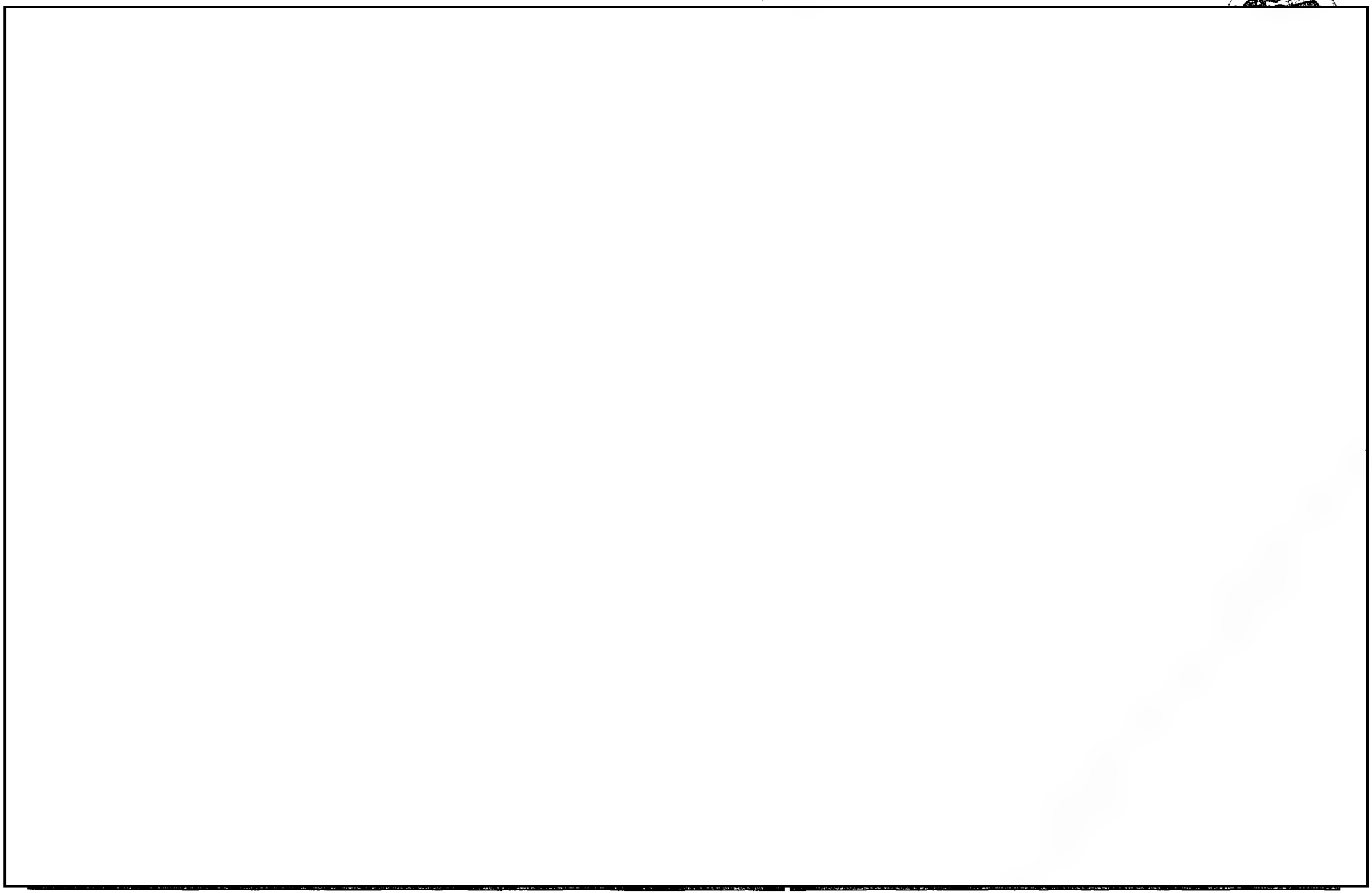


(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted] programs are special access programs and are not included in this brief.

(b)(3)-P.L. 86-36

If information is required, properly cleared members may request the data from NSA.

NSA/CSS "Footprint"

The NSA/CSS Extended Enterprise

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

NSA/CSS Extended Enterprise

Legend

NSA/CSS Washington

(U//~~FOUO~~) NSAHQ – NSA/CSS Headquarters, Fort Meade, MD

NSA/CSS Cryptologic Centers

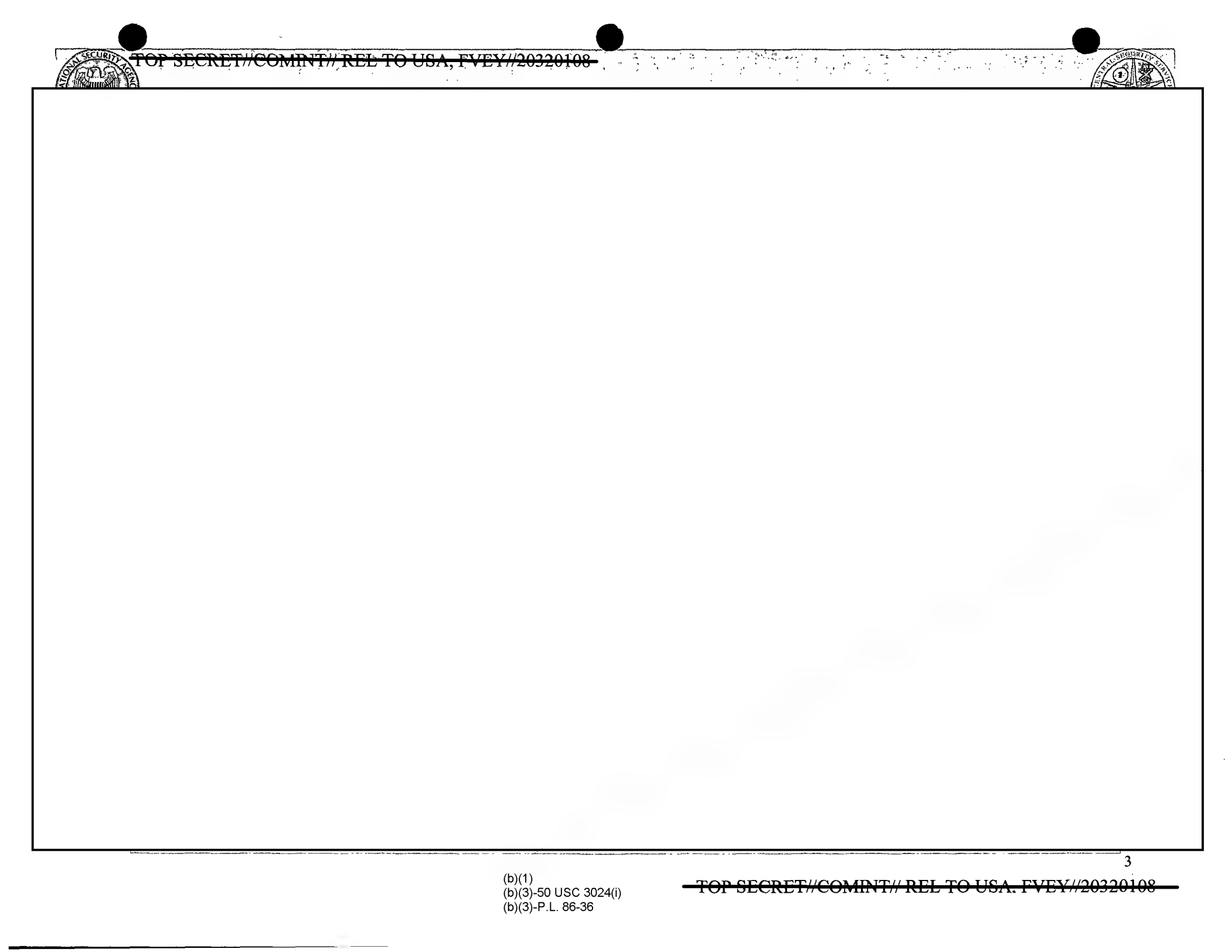
(U//~~FOUO~~) NSAC – NSA/CSS Colorado, Denver, CO
(U//~~FOUO~~) NSAG – NSA/CSS Georgia, Augusta, GA
(U//~~FOUO~~) NSAH – NSA/CSS Hawaii, Honolulu, HI
(U//~~FOUO~~) NSAT – NSA/CSS Texas, San Antonio, TX

Special U.S. Liaison Offices

(U//~~FOUO~~) SUSLOL – Special U.S. Liaison Office, London
(U//~~FOUO~~) SUSLOO – Special U.S. Liaison Office, Ottawa
(U//~~FOUO~~) SUSLOC – Special U.S. Liaison Office, Canberra

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

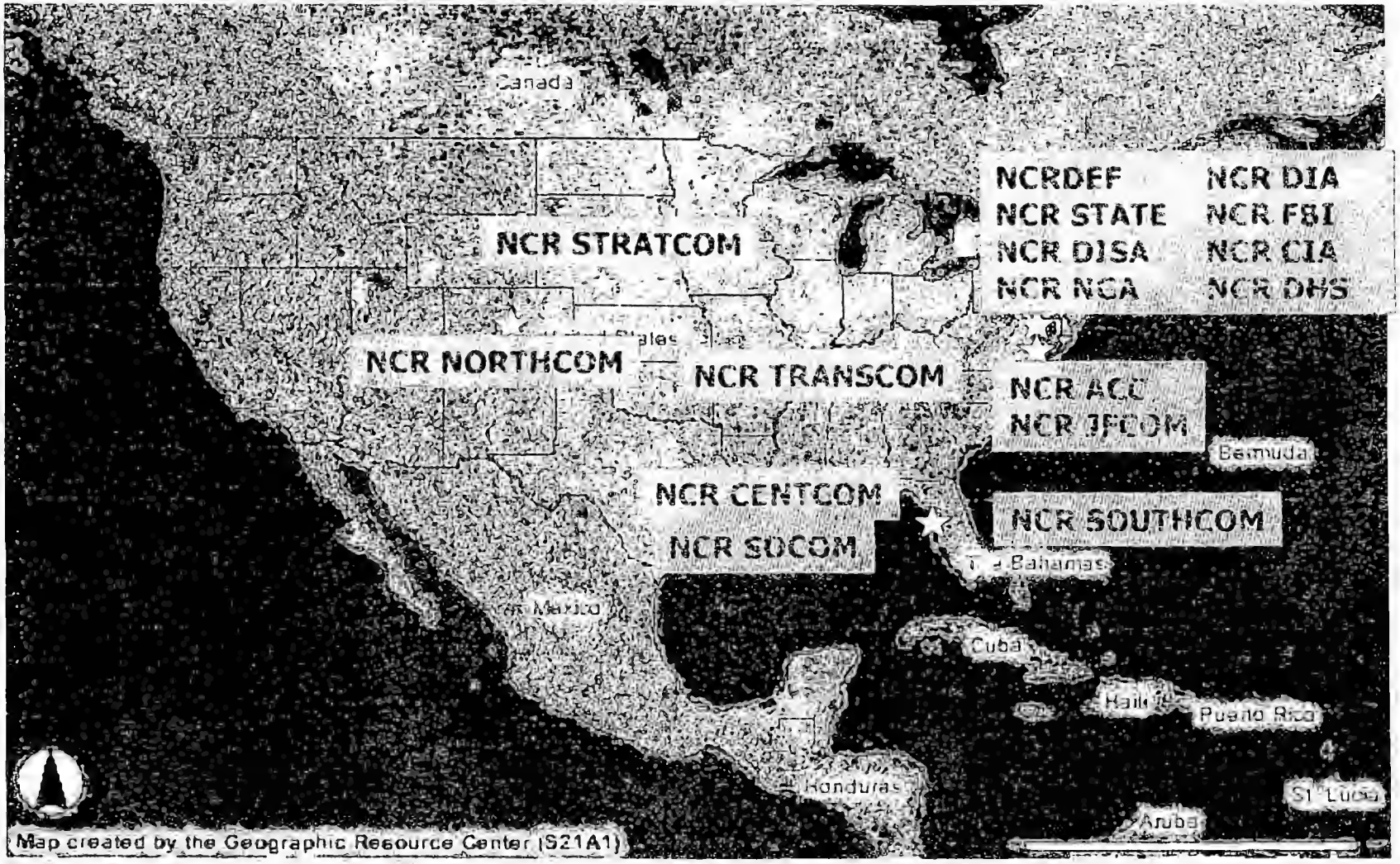
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

NSA/CSS Representatives

(Continental U.S.)



The Fort Meade NSA/CSS Campus

National Security Agency/
Central Security Service

(U) Cryptologic Center Build-Out: An Administration Transition Overview

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(S//SI)~~ In the early 1990s, in response to the changing customer requirements and communications environment following the end of the Cold War, NSA/CSS established Regional SIGINT Operations Centers (RSOC) in Georgia, Hawaii and Texas. They were spokes on the NSA wheel, connected to the headquarters facility in Maryland and to each other. The NSA/CSS workforce in those locations, housed on existing military bases and

~~(S//SI)~~ The years following September 11th brought several important changes to NSA/CSS that had a direct bearing on the RSOCs and how they were used. Specifically, NSA gained a heightened awareness of the need for mission assurance and continuity of operations planning (MA/COOP);

~~(S)~~ The Cryptologic Center (CC) build-out was one avenue to address these many changes.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

[redacted] The sites were matured from a tactical military support arm to a full extension of the NSA/CSS, a Cryptologic Center. The official nomenclature became NSA/CSS Colorado, Georgia, Hawaii, and Texas.

[redacted]

(U//~~FOUO~~) Detailed descriptions of each Cryptologic Center follow.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//39480914~~

NSA/CSS Georgia
COL John T. Owens III, Commander
Fort Gordon, Georgia

Mission: (U) As a leader in the net-centric cryptologic enterprise, NSA/CSS Georgia conducts SIGINT operations, trains the cryptologic workforce, and enables global communications, all critical to our national decision makers, Combatant Commands, and deployed U.S./Coalition forces.

(b)(3)-P.L. 86-36

(U) Aerial View of NSAG's Current Campus

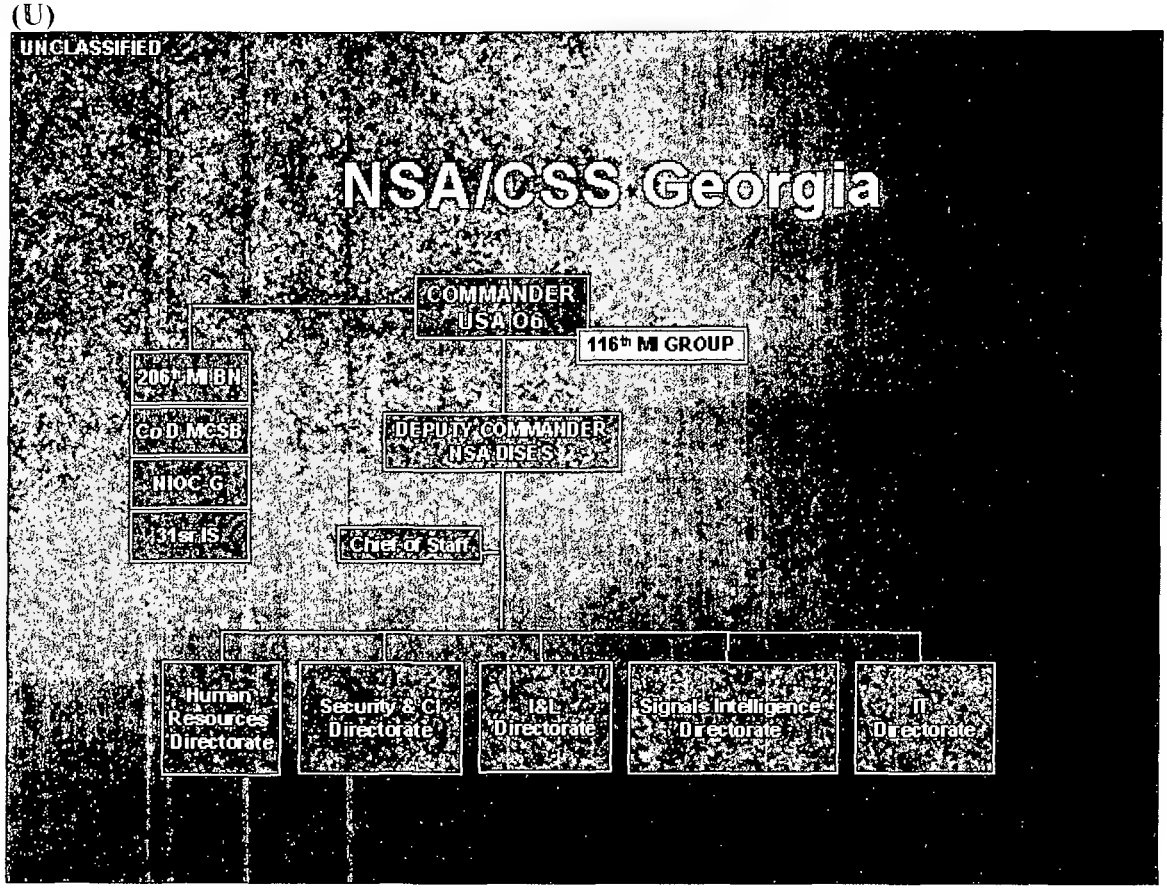
(U)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 39480914

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//39480914~~

Organizational Chart:

(U)



(U)

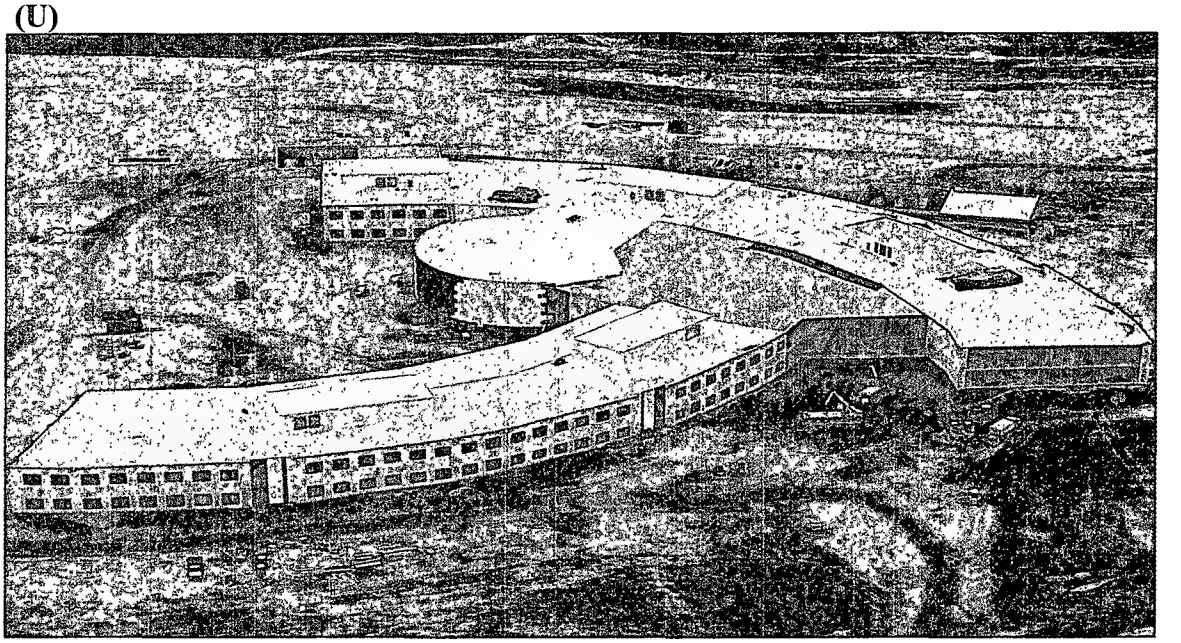
(U) Key Missions:

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

- (U) Collection Management in support of above targets
-
- (U) Information Sharing and Reporting

(U) MILCON:

(U)



(U)

Aerial view of the Sweet Tea construction site (Jul 2008)

(U) Sweet Tea Facility

- Size: 536,000 SF
- Groundbreaking: 26 Mar 2007
- Base Occupancy Date (BOD): Jun 2010
- Total Construction Cost: $525.85M
- New-space architecture provides a more open work environment that will:
  - Allow for greater collaboration within work centers
  - Provide greater flexibility for reconfiguring the workspace
    -

(U) Manpower (As of May 2008)

(U) 2008: 2,930

- NSA Civilians: 368
- Military: 2,173
- Service Civilians: 42
- Others (Foreign Party / IC Partners, Contractors): 347

(U) 2012: 4,319 (Projected)

- NSA Civilians: 686
- Military: 2,997
- Service Civilians: 46
- Others: 590

(U) 2015: 4,613 (Projected Total)

(U) NSAG Seat Requirements

- **2008**: 1,680
- **2012**: 2,428
- **2015**: 2,545

(U) Current NSAG Facilities

Approximate Gross Square Footage (GSF)

Building	GSF
• Back Hall	111,500
• MOD 2	72,000
• Georgia Center for Languages (GCL)	41,501
• GANNEX	41,501
• Group Component Headquarters (GCHQ)	24,100
• Navy Modular	20,000
• NSAG Warehouse	8,000
• GCHQ Annex	2,000

(//~~FOUO~~) IT:

- IT has programmed [redacted] for FY10-15 (b)(1) (b)(3)-P.L. 86-36
  - Covers the fit-up of 2,665 seats in Sweet Tea

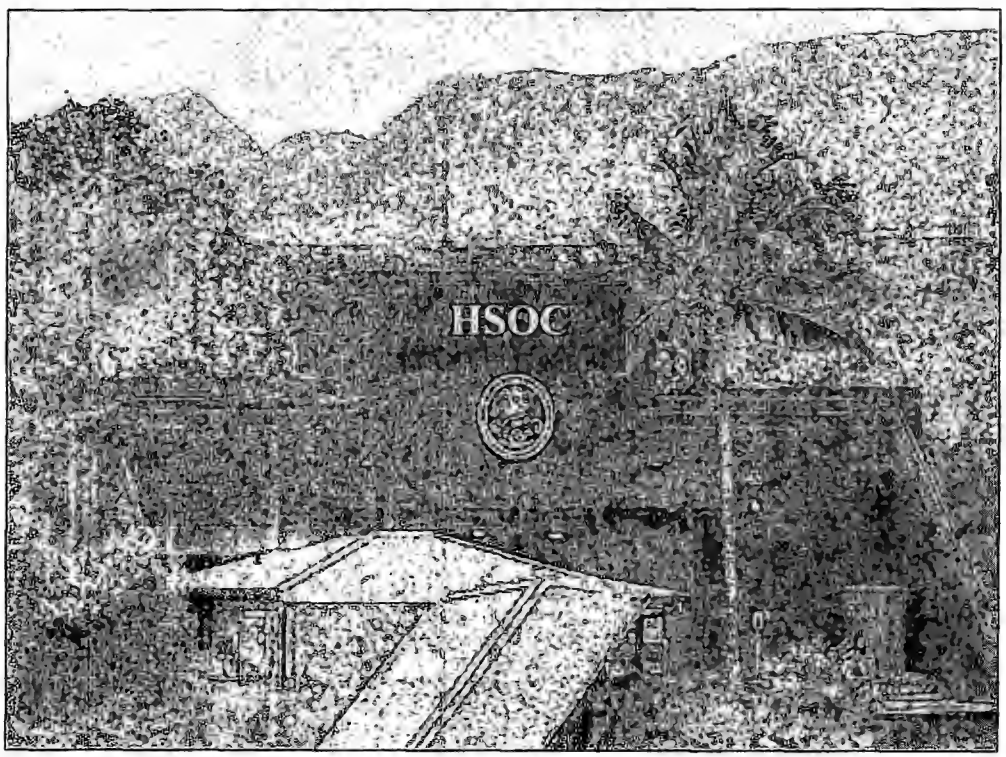
~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

NSA/CSS Hawaii

CAPT Jan Tighe, USN,
Commander
Kunia, Hawaii

Mission: (U) NSA/CSS Hawaii assures a decisive information advantage for our nation and allies to preempt, disrupt, or defeat adversaries and to protect our national interests by conducting relevant signals intelligence, information assurance, and network warfare operations.

(U)



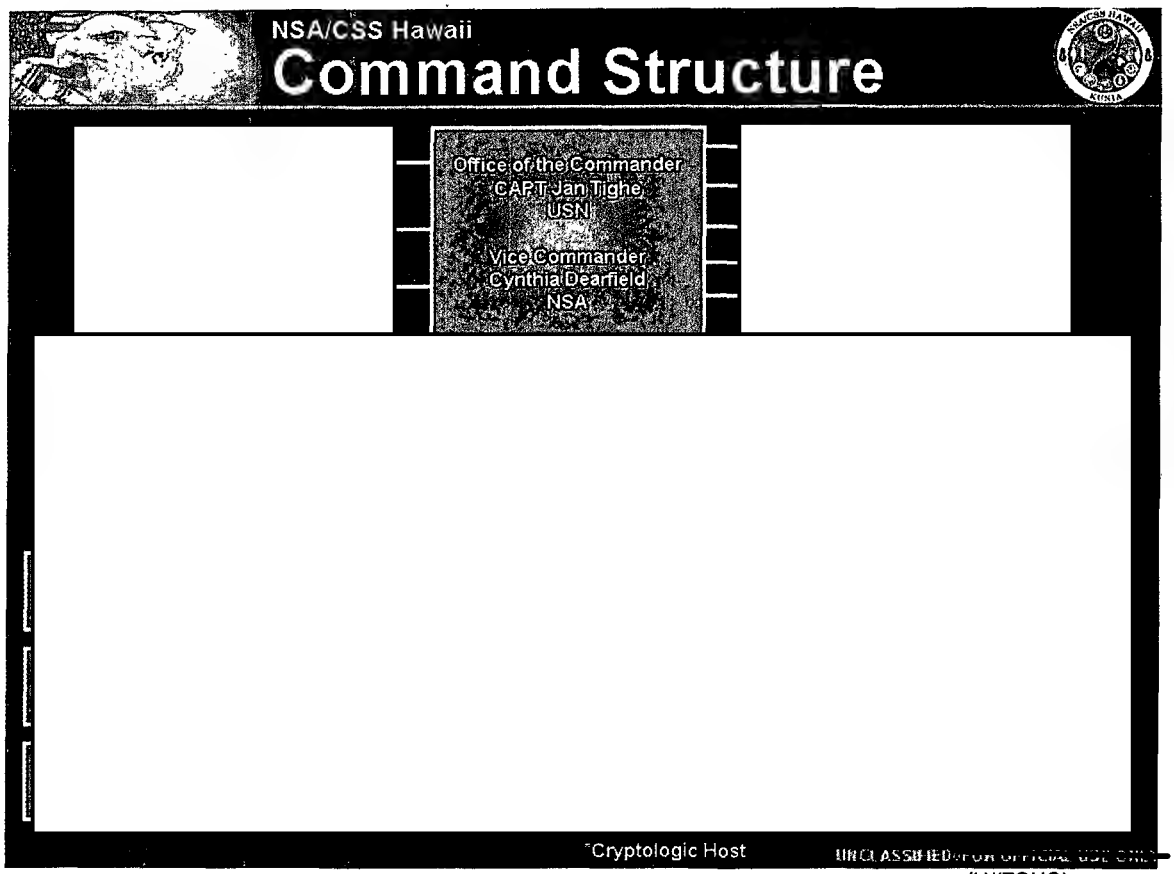
(U)

(U) NSA/CSS Hawaii
(U) Schofield Barrack, HI

~~(U//FOUO)~~

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108~~



(b)(3)-P.L. 86-36

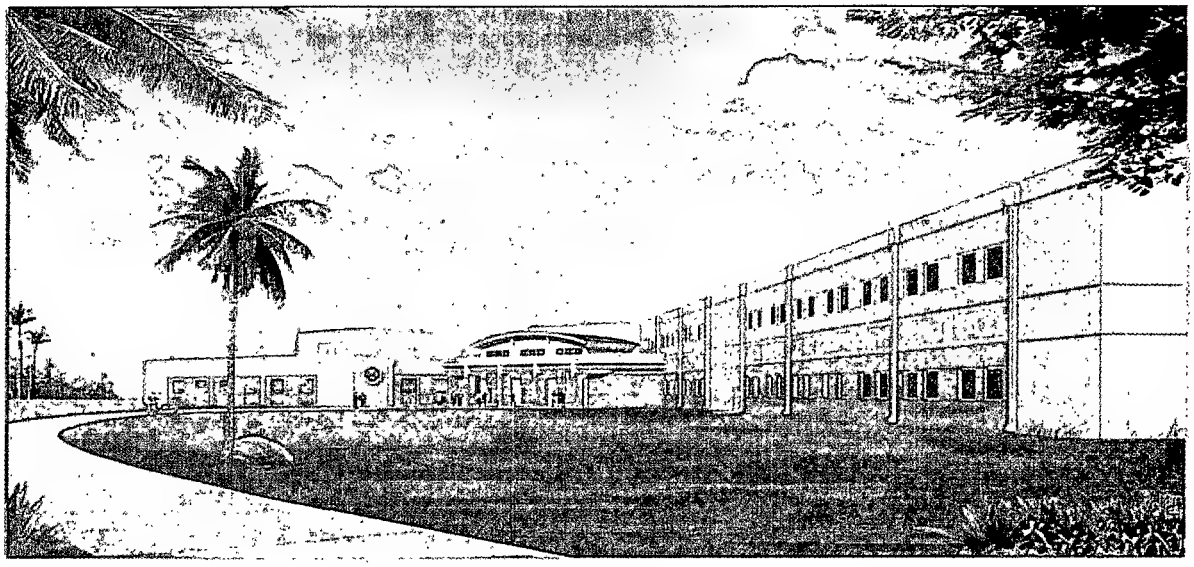
~~(U//FOUO)~~

~~(S//REL)~~ Key Missions:

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) MILCON:

(U)



(U) 1391 Approved by Congress: September 2006, $350.49M (U)
(U) Contract Awarded: 12 April 2007, $318.150M

(U) Groundbreaking Ceremonies: 30 August 2007
(U) Contract Completion Date: 2010

(U~~//FOUO)~~ Building Sizes:

- Operations Building: [redacted] Sq Ft (b)(3)-P.L. 86-36
- [redacted]

(U) Wahiawa Notional Seat Count: 1145

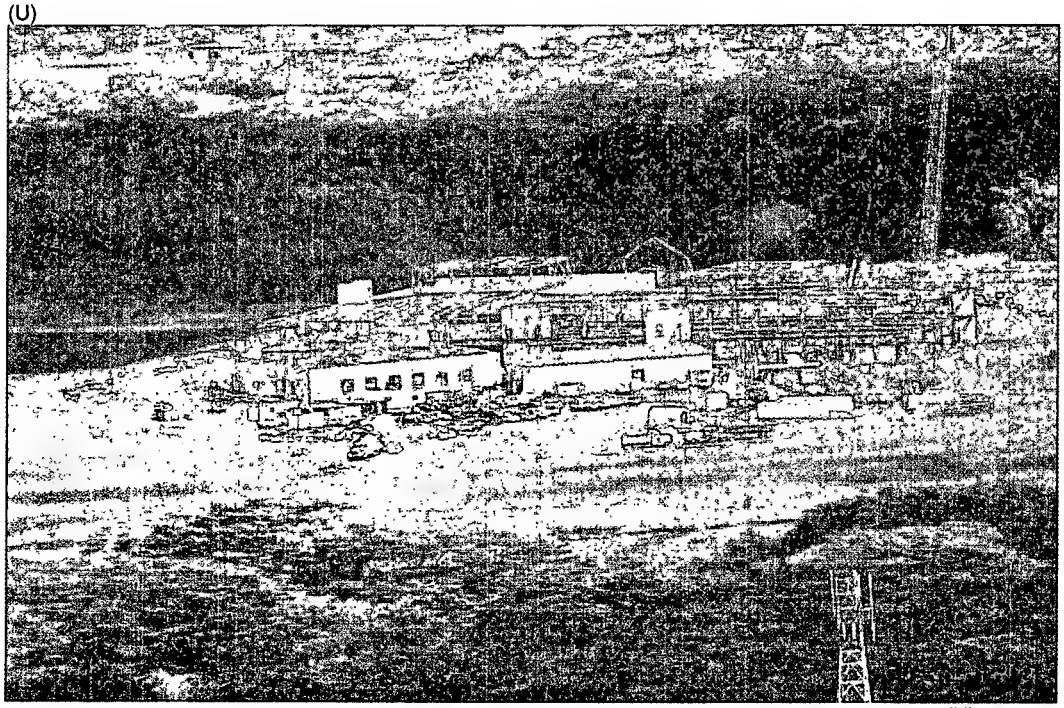
(U) New Open Space Architecture that will provide a more open work environment that will:

- Allow for greater collaboration within work centers
- Provide greater flexibility for reconfiguring the workspace

(U) Conference Rooms: 12
(U) VTC Rooms: 11
(U) Enclaves: 21

(U) Construction as of 29 August 2008

(U)



(U)

(U) Manpower (as of 22 August 2008)

(U) 2008: 3054
NSA Civilians: 224
Service Civilians: 121
Military: 2582
Other (Foreign Partners, IC Partners, Contractors): 127

~~(C//REL)~~

- [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(U) 2012: 4018 (projected)
NSA Civilians: 426
Service Civilians: 132
Military: 3240
Other: 180

(U) 2015: 4075 (projected)

(U) Seat Requirements

2008: 1550 (Kunia) + 350 [redacted] (b)(3)-P.L. 86-36
2012: 2625
2015: 2640

(U//~~FOUO~~) Training Space Requirements:

- Unclassified: 33,740 sq. ft.
- Classified: 32,560 sq. ft.

~~(S//REL)~~ Funded Resources: MILCON $370.49, IT Fit-up [redacted] FY10-15 (b)(1) (b)(3)-P.L. 86-36

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

NSA/CSS Texas
Col John Bansemer
Commander

Medina Annex, San Antonio, TX

Mission: (~~U//FOUO~~) NSA/CSS Texas conducts *Signals Intelligence* and *Computer Network Operations* worldwide, in support of National and tactical decision-makers, customers/partners. Applies geographic and functional expertise [redacted]

(b)(3)-P.L. 86-36

(U)

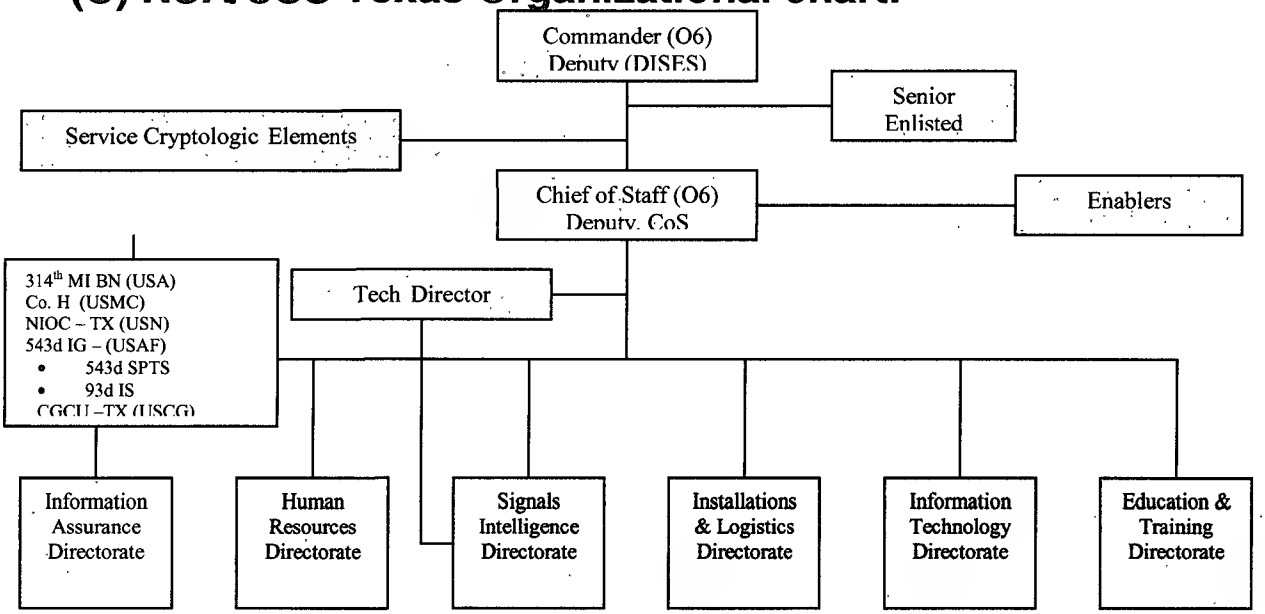
(U)

Aerial view of current NSA/CSS Texas campus at, Medina Annex

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

(U) NSA/CSS Texas Organizational chart:



Key Missions:

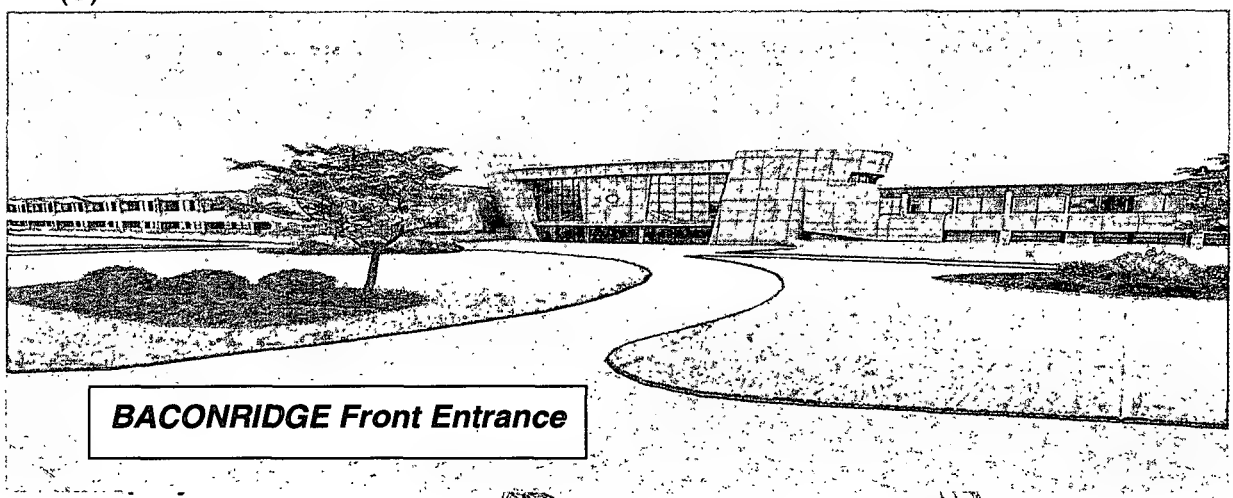
- (U) ICN (International Crime and Narcotics)

(b)(1)
(b)(3)-P.L. 86-36

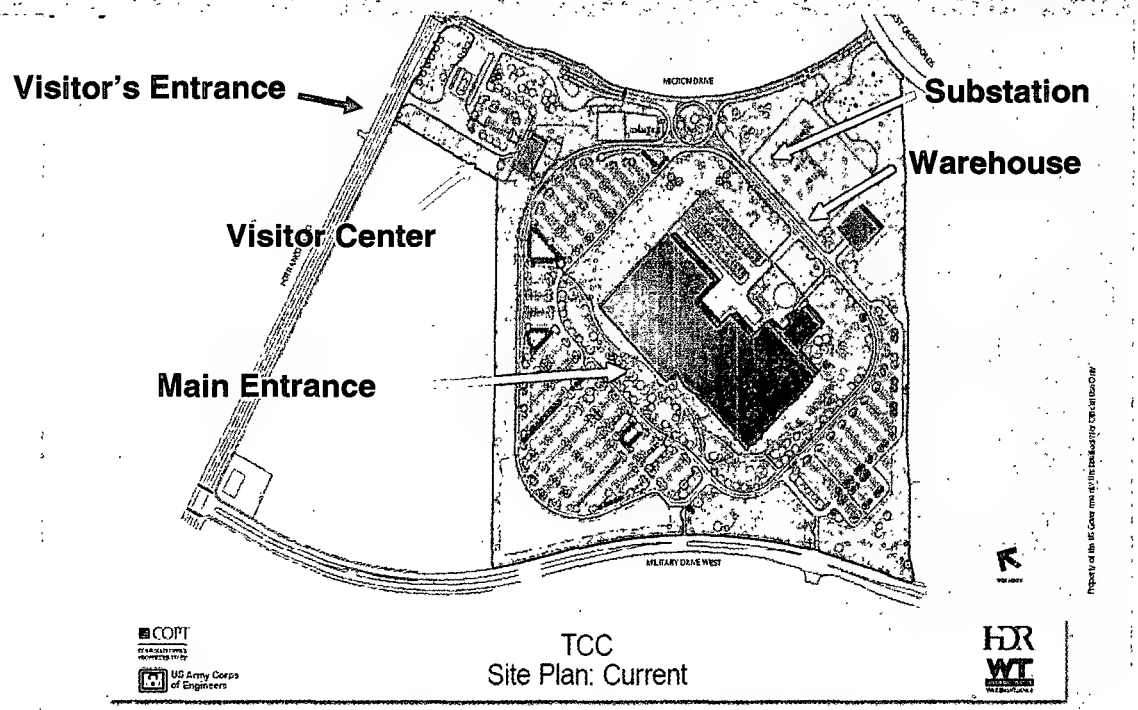
- (U) Computer Network Operations (CNO)
- (U) Information Sharing and Reporting

Facilities:

(U)



BACONRIDGE Front Entrance



(U)

Future NSAT Campus

(U) BACONRIDGE:

- (U) Leased Facility began Spring FY05
- (U) Renovation and Demolition began Fall FY05
- (U) Building Occupancy Date (BOD):
  - Bldg A: April 2010
  - Bldg B: April 2010

- (U) Vacate Medina Annex Sept 2014
- (U) Total SF – 469,000
  - Bldg A Seat Count: 1,229
  - Bldg B (Data Center)
- (U) New-space architecture provides a more open work environment that will:
  - Allow for greater collaboration within work centers
  - Provide greater flexibility for reconfiguring the workspace

(U) Manpower: (As of May 2008)

(U) 2008: 2,136
NSA Civilians: 246
Military: 1,689
Service Civilians: 56
Others (Foreign / IC Partners, Contractors): 145

(U) 2012: 3,405
NSA Civilians: 758
Military: 2,318
Service Civilians: 81
Others: 248

(U) 2015: 3,648 Projected

(U) NSAT Future Seat Requirements:

- **2012:** 1,903
- **2015:** 2,380

(U) IT:

(U) The Data Center is composed of 6 rooms, 3 of which belong to NSA/CSS Texas (Rooms 3,5, and 6) the remaining 3 belong to corporate NSA

(U) Delivered capacities at BOD

7,987 sf Comms Center (Room # 6) at 70 watts/sf
9,524 sf [redacted] (Room # 5), 383 watts/sf (b)(3)-P.L. 86-36
16,593 sf room # 3, 220 watts/sf

23,480 sf room # 1, 0 watts/sf
15,437 sf room # 2, 0 watts/sf
17,105 sf room # 4, 0 watts/sf

Capacities Post BOD
23,480 sf room # 1, 388 watts/sf
15,437 sf room # 2, 429 watts/sf

16,593 sf room # 3, 440 watts/sf
17,105 sf room # 4, 427 watts/sf

(U) Funding:

- Renovation and Fit-Up of Bldgs A & B (FY05-FY09) [redacted] (b)(3)-P.L. 86-36
- Sustainment and Lease Costs FY06-FY13: [redacted]
- IT Funding for FY10-15: [redacted] (covers 2,400 seats) (b)(1) (b)(3)-P.L. 86-36

NSA/CSS Colorado

Sara Mayfield
Director NSA/CSS Colorado
Aurora, Colorado
7 November 2008

Welcome: (U~~//FOUO)~~ NSA/CSS Colorado is the national headquarters for the Global Technical SIGINT (TechSIGINT) Enterprise (GTSE). TechSIGINT information includes Electronics INTelligence (ELINT), [redacted] Radio Frequency (RF) Communications Externals data associated with radars, missiles, aircraft, space systems, weapons systems, and selected information and communications systems worldwide. NSA/CSS Colorado provides leadership for all elements of the SIGINT Community performing collection, production and customer relations involving these programs.

(b)(3)-P.L. 86-36

(U~~//FOUO)~~ The Technical SIGINT Enterprise is a globally dispersed federation of collectors, producers and consumers of SIGINT product. While centrally managed from NSA/CSS Colorado, the Technical SIGINT mission is executed globally. [redacted]

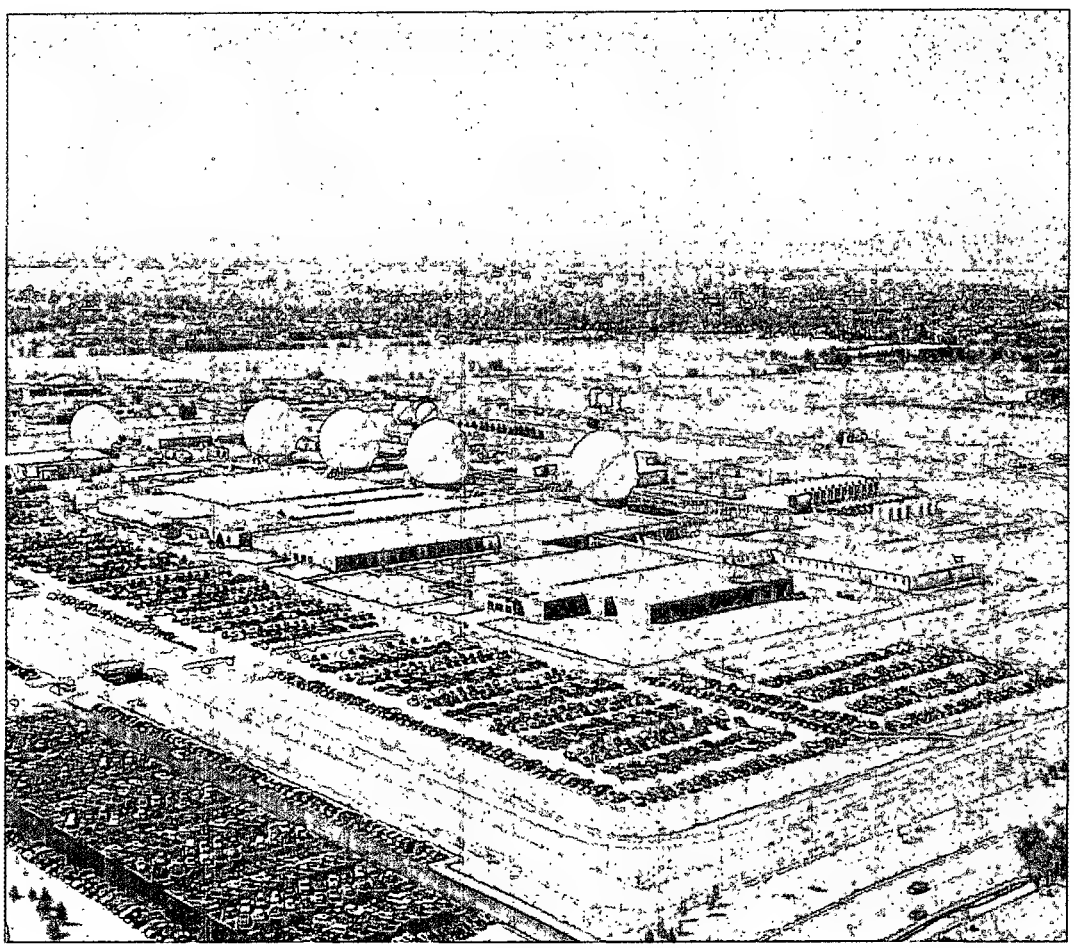
[redacted]

Mission: (U~~//FOUO)~~ As the sole NSA product line, W&S headquarters located outside of Fort Meade, NSA/CSS Colorado ensures the Global Technical SIGINT (TechSIGINT) Enterprise (GTSE) is synchronized -- mission responsibilities are deconflicted, all elements are aware of their own and each other's responsibilities and that customer Information Needs are met.

Vision: Partnered to achieve strategic and tactical advantage against our adversaries.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

NSAC

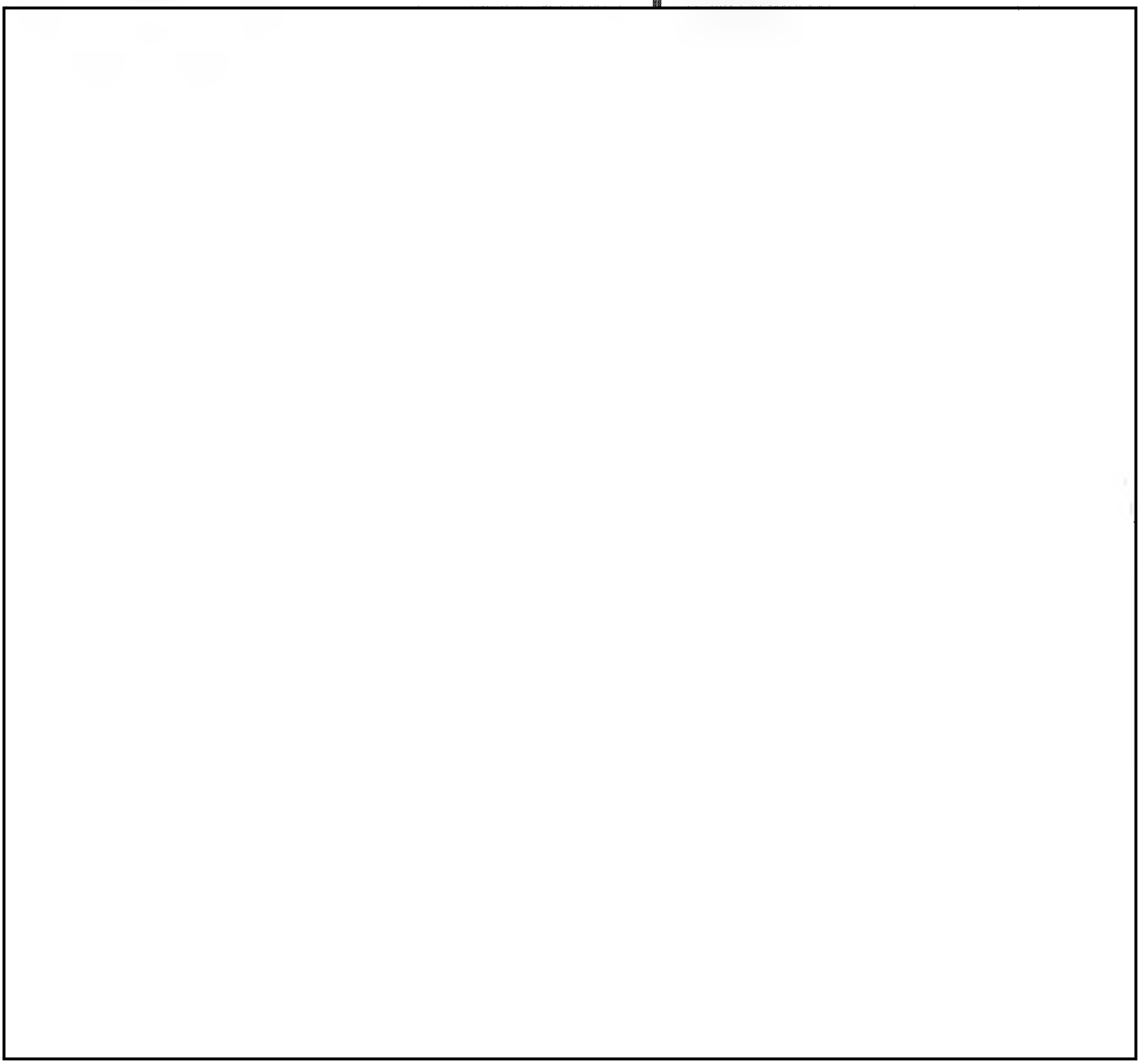


(b)(1)
(b)(3)-P.L. 86-36

NSA/CSS COLORADO ORGANIZATION CHART

Located in Colorado | Located in Maryland

Sara Mayfield
Director
Col Ken Nugent
Deputy Director



Missions:

~~(S//REL TO USA, FVEY)~~ Global TechSIGINT (ELINT [redacted] RF Communications Externals) Analysis and Production (b)(3)-P.L. 86-36

[redacted]

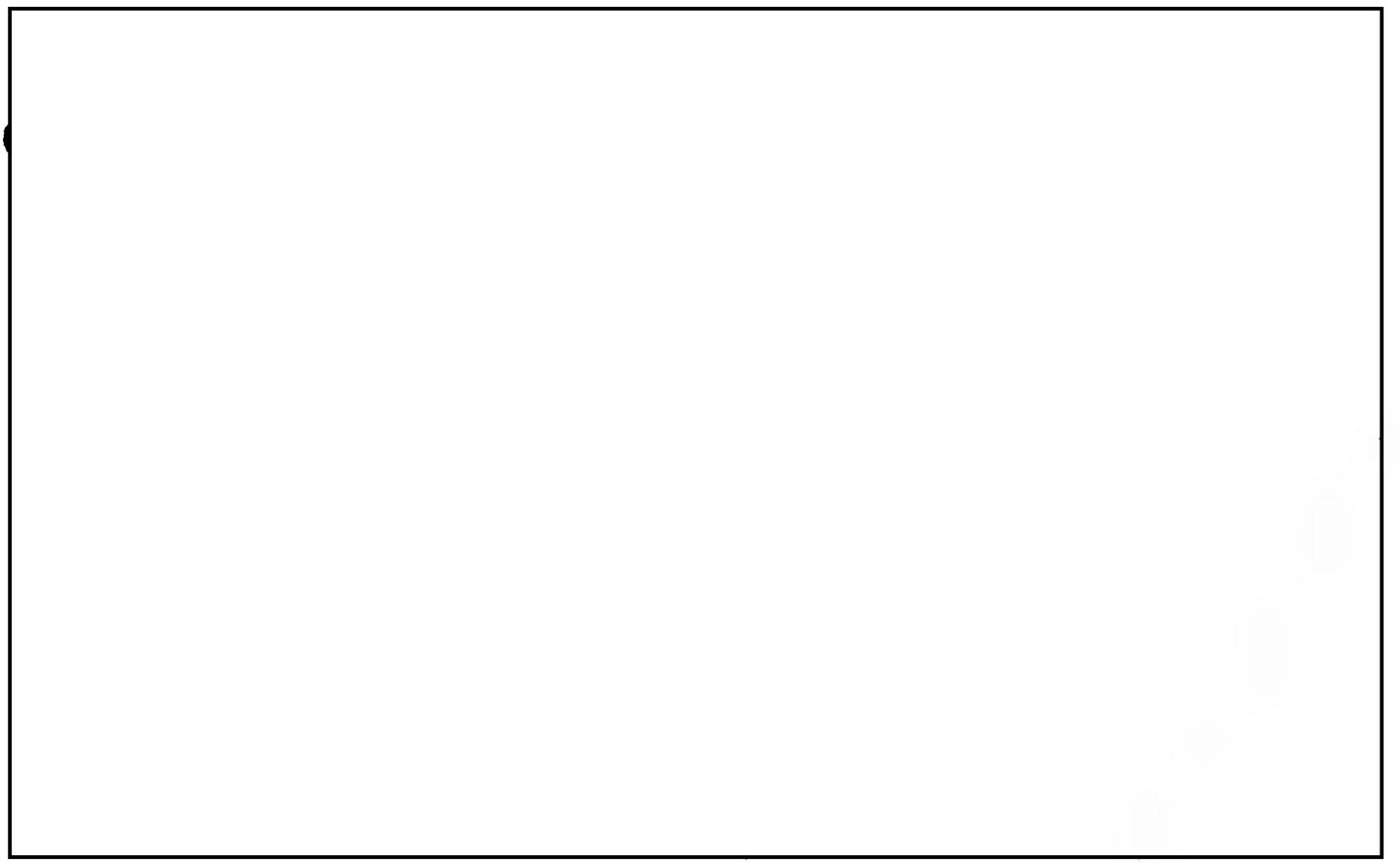
Manning:

~~(C//REL TO USA, AUS, CAN, GBR)~~ Manpower of NSA Civilian and multi-service Consolidated Cryptologic Program (CCP), Service Cryptologic Element (SCE) military personnel are augmented by USAF P2 personnel. Personnel at Field Station Denver (FSD) also support NSAC personnel. (b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

NSAC/FSD August 2008:

• NSA/CSS	Civilians	233		
• USA	Civilians	1	Military	287
• USN	Civilians	1	Military	258
• USAF	Civilians	2	Military	381
• USMC			Military	34
• USCG			Military	16
• Contractors		115		

NSAC/FSD TOTAL **1324**



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Accesses Through Foreign Partnerships

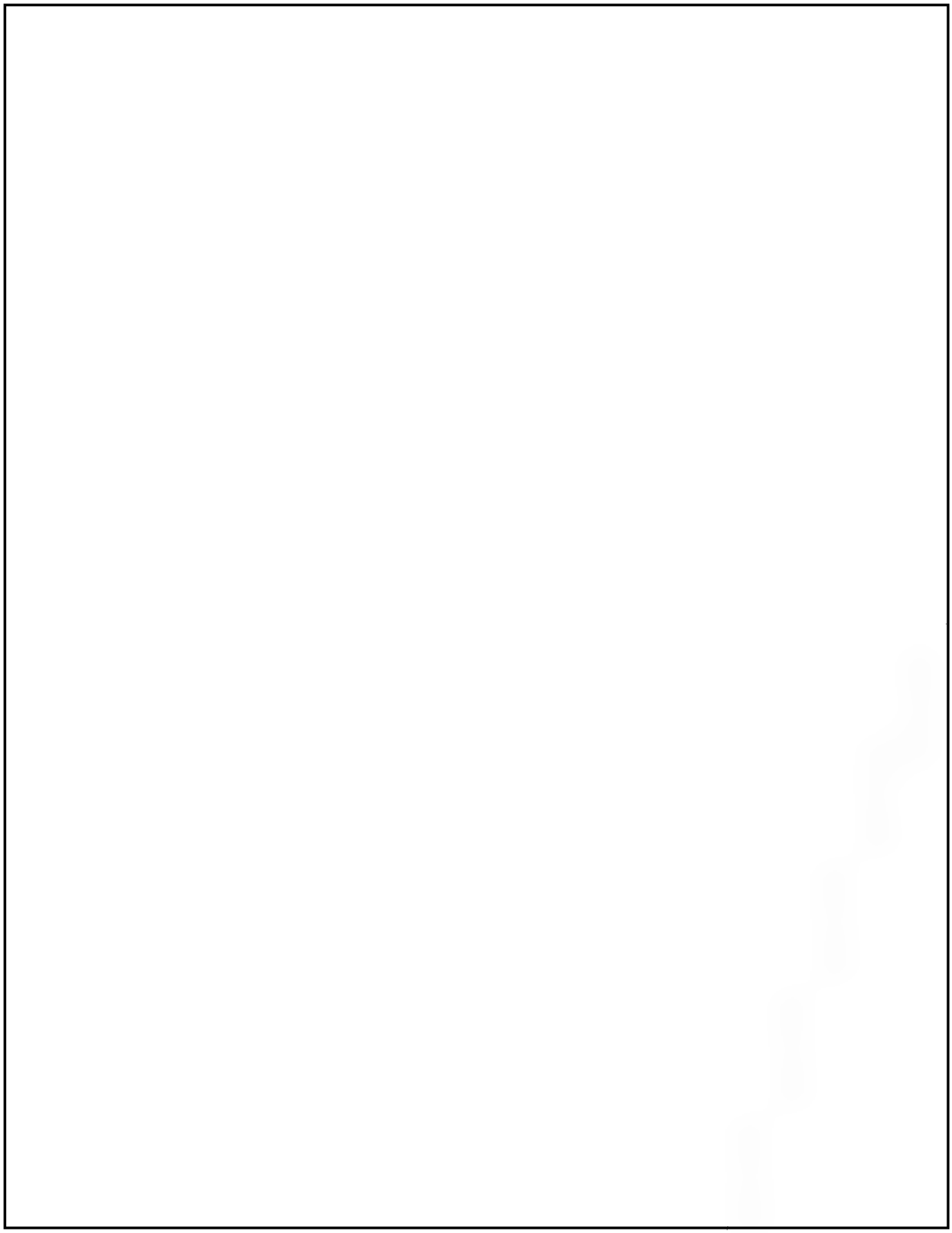
(U//~~FOUO~~) NSA/CSS's relationships with its foreign partners are unique within the Intelligence Community, and exist for one purpose: to further the goals of NSA/CSS, the Community, and the United States itself. Our foreign partnerships enable the Agency to achieve a truly global intelligence posture.

(b)(3)-P.L. 86-36

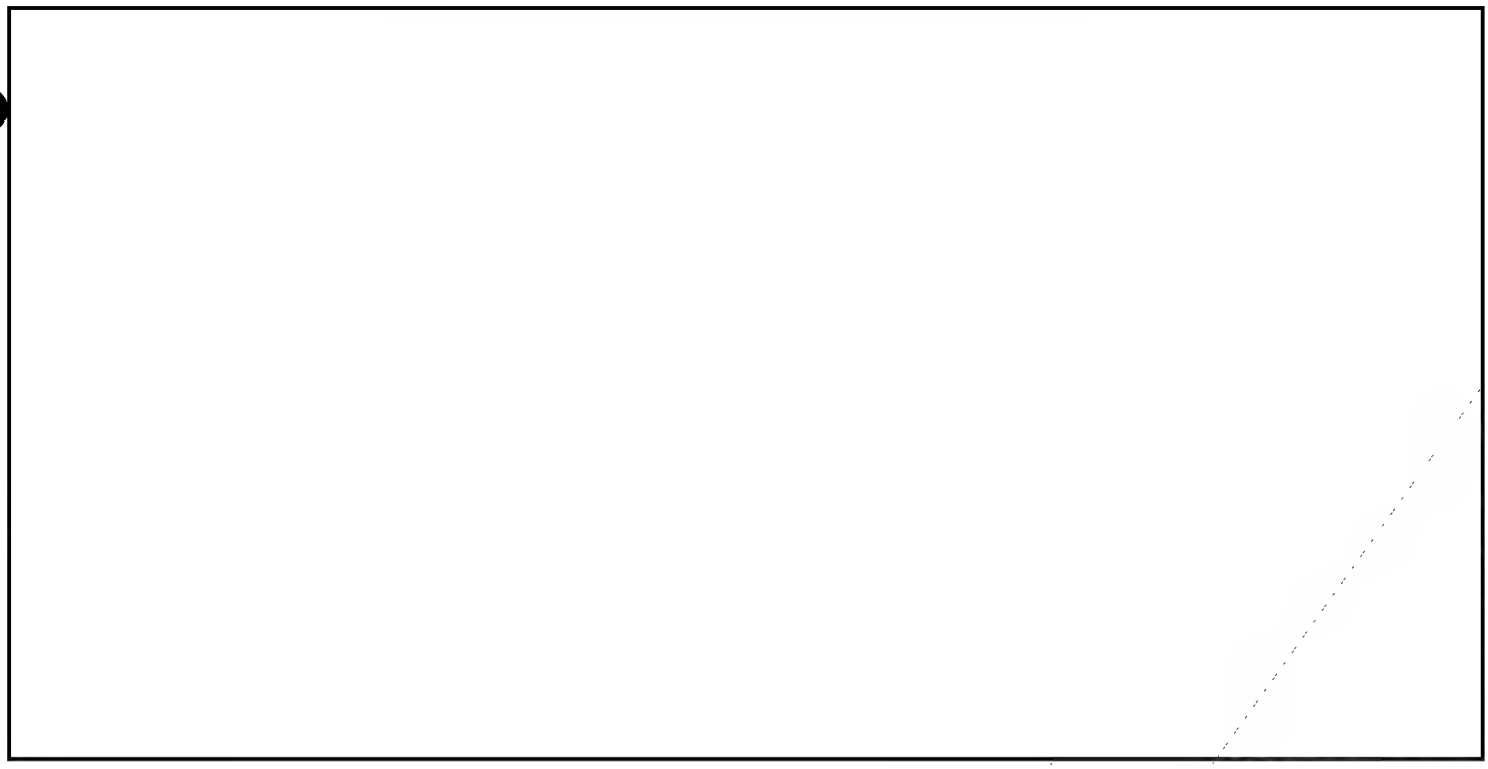
Signals Intelligence Partnerships

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36



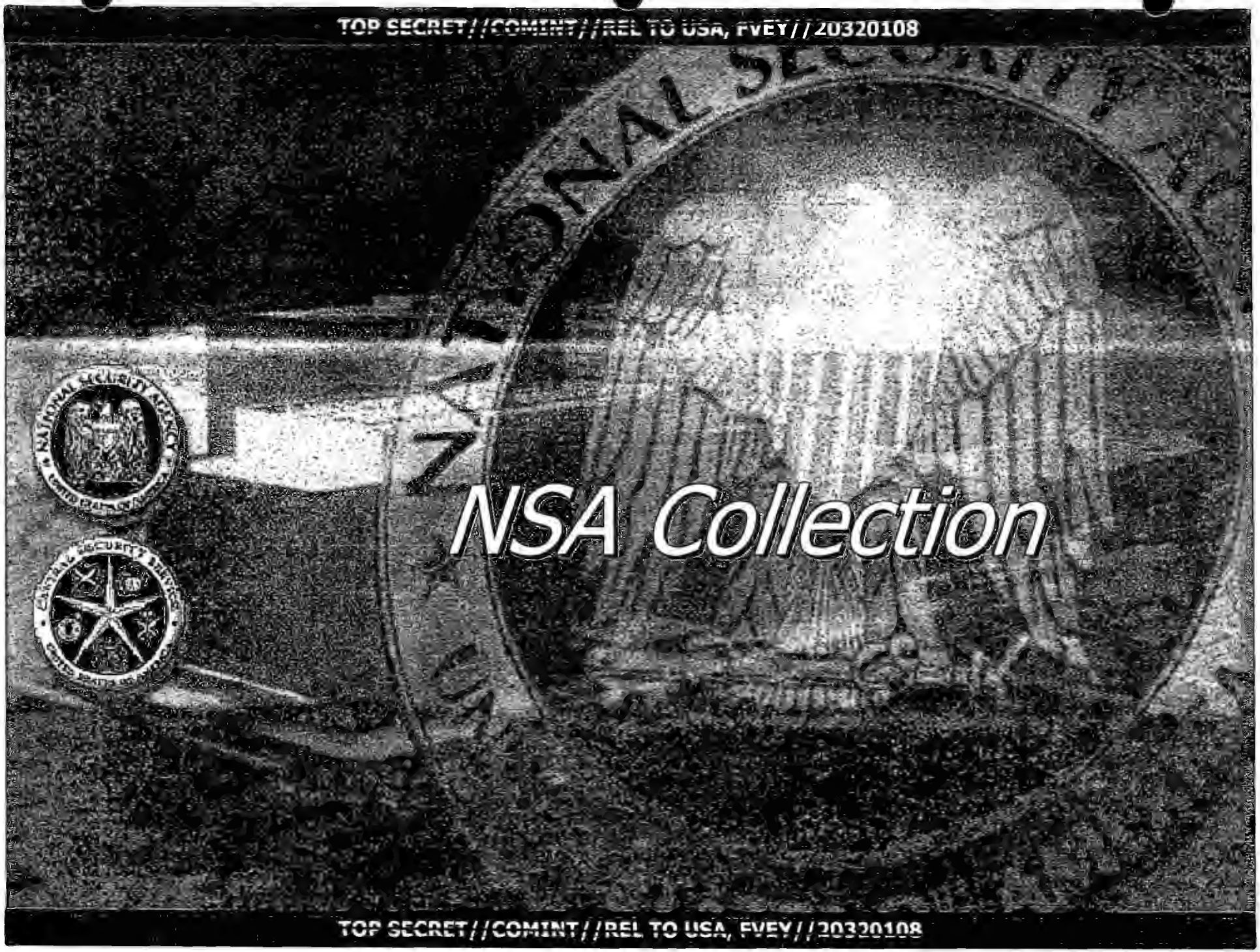
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Information Assurance Partnerships

~~(C//REL TO USA, FVEY)~~ With regard to NSA/CSS's Information Assurance (IA) partnerships, the unique benefits are not always obvious.

In addition, IA relationships enable NSA/CSS to ensure secure interoperability for the U.S. warfighter and the coalition operational environment. It is critical to our warfighters that we protect their entire communications infrastructure, the people doing the communicating, and the information being communicated. To achieve this objective we must make sure that our foreign partners are employing secure interoperability and infrastructure standards when engaged in operations with the U.S.

(b)(1)
(b)(3)-P.L. 86-36


NSA Collection

SERVING OUR CUSTOMERS

Major Finished Intelligence Producers:

CIA
DIA
State/INR
NGA
National Intelligence Council

Policymakers/ Law Enforcement:

White House
Cabinet Officers
Director National Intelligence
U.S. Ambassadors
U.S. Trade Representative
Congress
Departments of:
Homeland Security
Agriculture
Justice
Treasury
Commerce
Energy
State

Military/Tactical:

JCS
Combatant Commanders
Task Forces
Tactical Commands
All Military Services
Department of Defense

Alliances
[redacted]
NATO

(b)(3)-P.L. 86-36

SIGINT Targets

SIGINT Challenges

Complex Target Environment

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

The World We Must Master

This Environment Never Stops Accelerating, Evolving, Expanding

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

- Allies and adversaries live and work on the same network
- Defending and exploiting this shared space is our primary mission (b)(3)-P.L. 86-36

We must go 'stride for stride' with our targets through continued integration and modernization, supported by robust IT and PSC

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

Data Acquisition Activities

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

A balanced portfolio is needed to address SIGINT collection and processing requirements.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Global NSA/CSS Collection Access

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

FOREIGN SIGINT PARTNERS

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

The National Security Agency

CHIEF OF STAFF
Deborah A. Bonnani

DEPUTY CHIEF CSS
Brig Gen Noel T. "Tom" Jones, USAF

DIRECTOR
BUSINESS MGMT INTEGRATION
Mary P. (Terri) Fyock

DIRNSA
(Chief CSS Commander JFCC-NW)
LTG Keith B. Alexander, USA

DEPUTY DIRECTOR
Mr. John (Chris) Inglis

INSPECTOR GENERAL
George Ellard

GENERAL COUNSEL
Vito T. Potenza

EEO
Linda M. Grimm

DIRECTOR'S SCIENCE ADVISOR
Dr. James E. Heath

DIRECTOR
SIGNALS INTELLIGENCE
William M. Crumm

DIRECTOR
INFORMATION ASSURANCE
Richard C. Schaeffer, Jr.

DEPUTY DIRECTOR
JFCC-NW
Brig Gen Suzanne M. Vautrinot, USAF

DIRECTOR
RESEARCH
Dr. James R. Schatz

CHIEF
TECHNOLOGY OFFICER
Dr. Prescott B. Winter

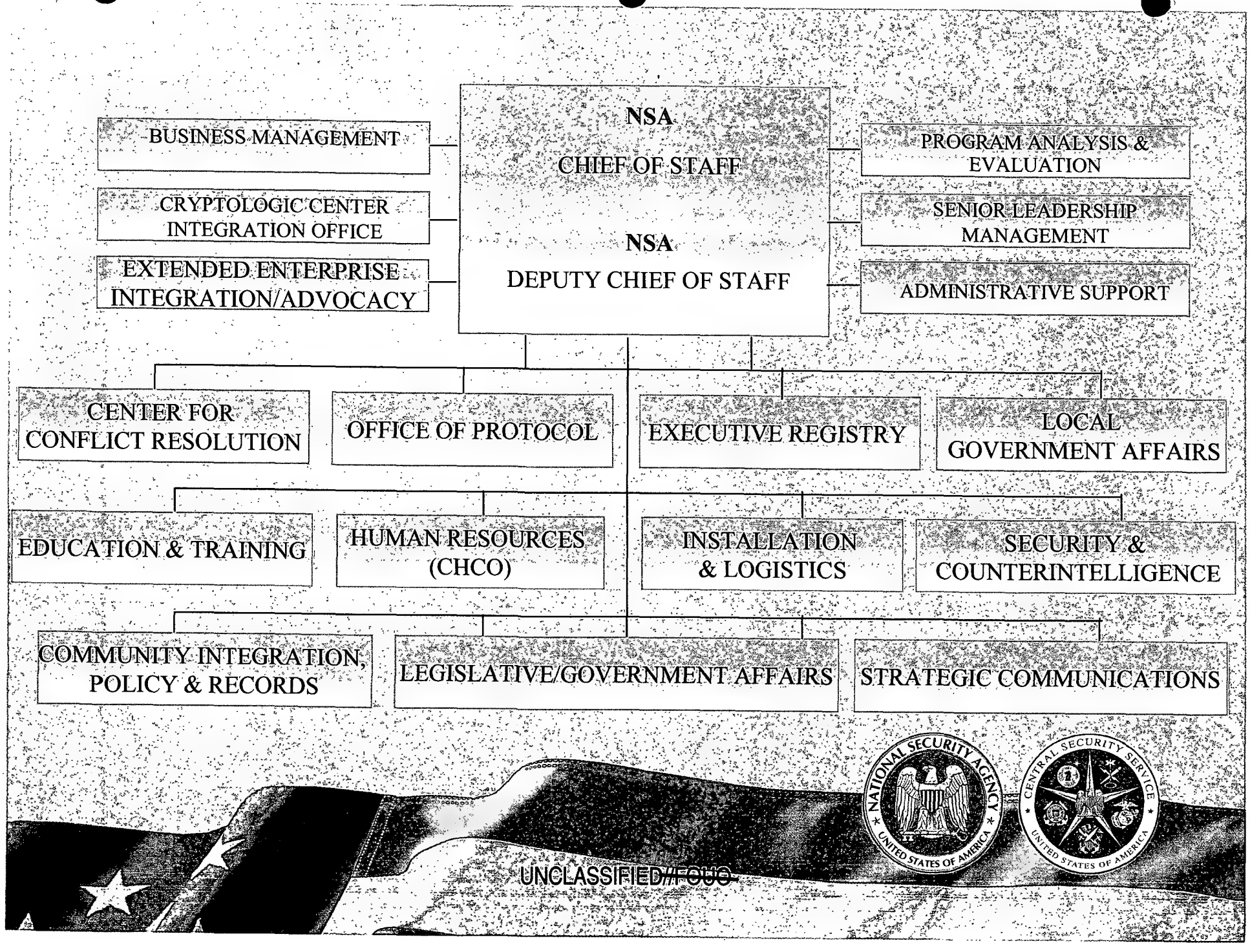
DIRECTOR FOREIGN AFFAIRS – James M. Cusick

DIRECTOR NSA/CSS Threat Operations Center (NTOC) William P.Marshall

DIRECTOR NSA/CSS Commercial Solutions Center (NCSC) – Curtis W. Dukes

DIRECTOR National Security Operatons Center (NSOC) – RDML Norman Hayes

UNCLASSIFIED//FOUO


NSA
CHIEF OF STAFF
NSA
DEPUTY CHIEF OF STAFF
BUSINESS MANAGEMENT
CRYPTOLOGIC CENTER INTEGRATION OFFICE
EXTENDED ENTERPRISE INTEGRATION/ADVOCACY
PROGRAM ANALYSIS & EVALUATION
SENIOR LEADERSHIP MANAGEMENT
ADMINISTRATIVE SUPPORT
CENTER FOR CONFLICT RESOLUTION
OFFICE OF PROTOCOL
EXECUTIVE REGISTRY
LOCAL GOVERNMENT AFFAIRS
EDUCATION & TRAINING
HUMAN RESOURCES (CHCO)
INSTALLATION & LOGISTICS
SECURITY & COUNTERINTELLIGENCE
COMMUNITY INTEGRATION, POLICY & RECORDS
LEGISLATIVE/GOVERNMENT AFFAIRS
STRATEGIC COMMUNICATIONS
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
CENTRAL SECURITY SERVICE
UNITED STATES OF AMERICA
UNCLASSIFIED//~~FOUO~~

Customers

50+ National Level customers arrayed into four primary "Pillars of Support"

POLICY

- US / UN
- State
- White House NSC
- DOT / FAA
- Federal Reserve
- FCC
- FDIC
- Export-Import Bank
- NRC
- Agriculture
- Energy
- Interior
- Treasury
- Commerce
- USTR
- Labor
- Health & Human Svcs
- EPA
- NASA

MILITARY

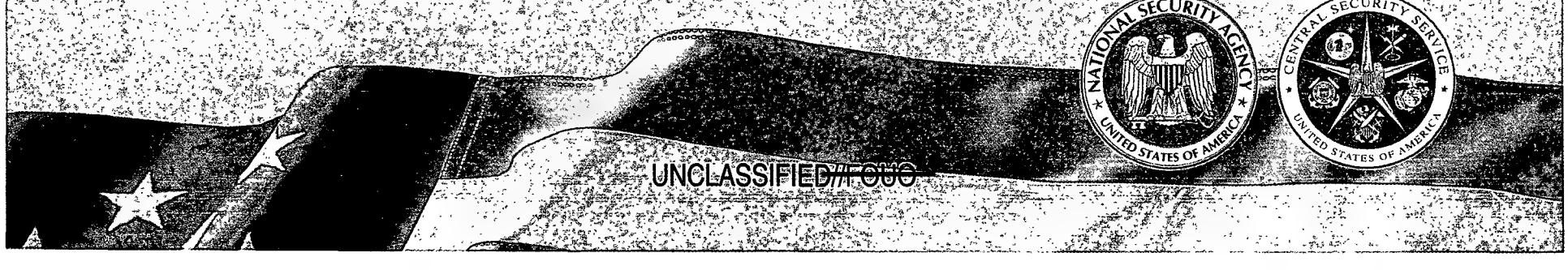
- Navy
- Marines
- Air Force
- Army
- DIA
- NASIC
- NGIC
- OSD
- JCS
- National Guard
- DISA
- DTRA
- MDA
- CENTCOM
- NORTHCOM
- EUCOM
- NATO
- TRANSCOM
- PACOM
- SOUTHCOM
- SOCOM
- STRATCOM
- JFCOM

INTELLIGENCE PARTNERS

- CIA
- NGA
- NRO
- ODNI
- NCTC

LAW ENFORCEMENT AND HOMELAND SECURITY

- DoJ
- ATF
- DEA
- FBI
- US Marshals
- DHS
- TSA
- ICE
- CBP
- Secret Service
- Coast Guard



NSA/CSS Leadership Biographies

Director, NSA; Chief, CSS; Commander, JFCC-NW

Deputy Director, NSA

Chief of Staff

Information Assurance Director

Signals Intelligence Director

Deputy Commander, JFCC-NW

Deputy Chief, CSS

General Counsel

Inspector General

Director's Science Advisor

Director, Equal Employment Opportunity and Diversity

Director, Business Management Integration

Associate Director, Global Integration Office

Associate Director, Strategic Communications

Associate Director, Community Integration, Policy, and Records

Associate Director, Senior Leadership Management

Deputy Chief of Staff, Strategic Issues

Director, National Security Operations Center

Director, NSA/CSS Threat Operations Center

Director, NSA/CSS Commercial Solutions Center

Director of Technology; Chief Technology Officer; Chief Information Officer

Director for Research

Deputy Director for Resources Management; Chief Financial Manager

Deputy Chief Financial Manager; Comptroller

Senior Acquisition Executive

Director, Foreign Affairs

Associate Director, Human Resources

Associate Director, Installation and Logistics

Associate Director, Legislative Affairs

Associate Director, Education and Training

Associate Director, Security and Counterintelligence

Director, Program Analysis and Evaluation

LTG Keith B. Alexander, United States Army

Lieutenant General Keith B. Alexander, USA, is the Director, National Security Agency/Chief, Central Security Service (NSA/CSS) and Commander, Joint Functional Component Command - Network Warfare (JFCC-NW), Fort George G. Meade, MD. As the Director of NSA and Chief of CSS, he is responsible for a Department of Defense agency with national foreign intelligence and combat support responsibilities. NSA's civilian and military personnel are stationed worldwide. As Commander, JFCC-NW, he is responsible to plan, execute and manage forces for coordinating DoD computer network Attack (CNA) and computer network defense (CND) as directed by USSTRATCOM.

He was born in Syracuse, NY, and entered active duty at the U.S. Military Academy at West Point.

Previous assignments include the Deputy Chief of Staff (DCS, G-2), Headquarters, Department of the Army, Washington, DC; Commanding General of the U.S. Army Intelligence and Security Command at Fort Belvoir, VA; Director of Intelligence, United States Central Command, MacDill Air Force Base, FL.; and Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, for the Joint Chiefs of Staff. LTG Alexander has served in a variety of command assignments in Germany and the United States. These include tours as Commander of Border Field Office, 511th MI Battalion, 66th MI Group; 336th Army Security Agency Company, 525th MI Group; 204th MI Battalion; and 525th MI Brigade.

Additionally, LTG Alexander held key staff assignments as Deputy Director and Operations Officer, Army Intelligence Master Plan, for the Deputy Chief of Staff for Intelligence; S-3 and Executive Officer, 522nd MI Battalion, 2nd Armored Division; G-2 for the 1st Armored Division both in Germany and Operation DESERT SHIELD/DESERT STORM in Saudi Arabia.

LTG Alexander holds a Bachelor of Science degree from the U.S. Military Academy and a Master of Science degree in Business Administration from Boston University. He holds a Master of Science degree in Systems Technology (Electronic Warfare) and a Master of Science degree in Physics from the naval Post Graduate School. He also holds a Master of Science degree in National Security Strategy from the National Defense University.

His military education includes the Armor Officer Basic Course, the Military Intelligence Officer Advanced Course, the U.S. Army Command and General Staff College, and the National War College.

His badges include the Senior Parachutist Badge, the Army Staff Identification Badge, and the Joint Chief of Staff Identification Badge.

Mr. John C. (Chris) Inglis
Deputy Director for the National Security Agency

Current Position: Mr. Inglis took the position of Deputy Director of the National Security Agency in August 2006. As the senior civilian at NSA, he acts as the Agency's chief operating officer, guiding and directing strategies and policy, and serves as the principal advisor to the Director.

Major Assignments and Dates/Summary of Earlier Experience

- 2003-2006 Special United States Liaison Officer London
- 2001-2003 Signals Intelligence Deputy Director for Analysis and Production
- 1999-2001 Chief, Office of China and Korea, Operations Directorate
- 1998-1999 Deputy Chief, Office of China and Korea, Operations Directorate
- 1997 Promoted to the Senior Executive Service
- 1996-1997 Senior Operations Officer, National Security Operations Center
- 1995-1996 Deputy Chief within the Office of Policy
- 1992-1995 Participant in Senior Cryptologic Executive Development Program Management and Staff tours in the Directorates of Operations (SIGINT Production), Information Systems Security, and Plans and Programs
- 1991-1992 Visiting Professor, Department of Computer Science and Electrical Engineering, U.S. Military Academy (West Point, NY)
- 1986-1991 Information Security Analyst and Manager up through division level within NSA's Information Systems Security Directorate
- 1976-1985 U.S. Air Force Officer and Pilot
- 1985-2006 Brigadier General in the Air National Guard and qualified as a command pilot. Has commanded at Flight, Squadron, Group and Joint Force Headquarters.

- Past President NSA International Affairs Institute; Human Resources Management Association

Education:

- 1976 Graduated U.S. Air Force Academy, B.S. in Engineering Mechanics (Distinguished Graduate)
- 1977 Graduated Columbia University, MS in Mechanical Engineering (Guggenheim Fellow)
- 1984 Graduated Johns Hopkins University, MS in Computer Science
- 1990 Graduated George Washington University, Professional Degree in Computer Science
- 1996 Graduate of Air War College, USAF Squadron Officers School, Air Command and Staff College (Seminar)

Significant Awards:

- 1984 Clement's Award as the U.S. Naval Academy's Outstanding Military Faculty Member
- 1992 Department of Army Outstanding Civilian Service Award
- 1996 *Deputy Director of Operations Special Recognition Award*
- 2000 Presidential Rank Award for Meritorious Service
- 2001 Deputy Director of Operations Special Recognition Award
- 2002 Exceptional Civilian Service Award
- 2004 Presidential Rank Award for Distinguished Service

Personal Data:

(b)(6)

CURRENT POSITION: In February 2006, Ms. Deborah A. Bonanni was selected as the Chief of Staff at the National Security Agency, Department of Defense, Fort Meade, Maryland. The Chief of Staff organization is a corporate staff that exercises operational control over the corporate functions of Policy, Strategic Planning and Performance, External Relations and Communications, Field Advocacy, the Counterintelligence Center, and Corporate Management Services. The Chief of Staff also provides administrative support for the General Counsel, EEO, IG and the NSA Principal Directors.

EDUCATION: Ms. Bonanni received her Bachelor of Arts Degree Summa Cum Laude from Hood College in 1978 with a double major in History and Political Science. She received her Juris Doctorate from the Columbus School of Law at the Catholic University of America in 1982. She is a member of the Bars of both Maryland and District of Columbia.

PRIOR POSITIONS: Ms. Bonanni began her public service career as an attorney within the NSA Office of General Counsel (OGC). For the first ten years of her career, she served in positions of increasing responsibility within the OGC. In the mid-1990's, she embarked on a series of managerial positions outside the legal domain, and earned high marks for her ability to motivate and recruit highly talented people and to create organizations focused on customers, innovation, and performance. As the Chief, Human Resources Services, from 1996-2000, she led a series of new initiatives aligned with the strategic vision of the Director, NSA, designed to transform recruitment, retention, and recognition of the Agency's workforce. In 2001, she attended the Foreign Service Institute's Senior Seminar, a prestigious Department of State leadership program attended by top senior executives from the federal foreign affairs community. From 2002 until February 2006, she served as the Associate Director, Education and Training; the Training Director National Security Agency/Central Security Service (TDNC); and the Commandant of the National Cryptologic School. As the Associate Director, Ms. Bonanni had responsibility for the strategic direction, leadership and oversight of all education, training and professional development affecting the military and civilian members of the NSA/CSS workforce. Her primary goal was to ensure the delivery of exemplary, mission-relevant learning opportunities that yield the greatest return on investment for the NSA/CSS

enterprise and its key partners. As the Commandant, she was responsible for the daily operation of the National Cryptologic School, a nationally recognized academic institution providing tailored training and professional development services at NSA Headquarters, and throughout the enterprise.

PROFESSIONAL BACKGROUND: Ms. Bonanni became a member of the Defense Intelligence Senior Executive Service in 1997, and was recognized with the Presidential Rank Award, Meritorious Executive in 2000 and again in 2006. She is the recipient of the Exceptional Civilian Service Award, NSA's highest honorary award for exceptional leadership. In June 2001 she completed the Foreign Service Institute's Senior Seminar, a prestigious Department of State leadership program attended by top senior executives from the federal foreign affairs community.

PERSONAL: [redacted] (b)(6)

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied

(b)(3)-P.L. 86-36
(b)(6)

Page Denied